Univerzita Karlova

Filozofická fakulta

Ústav informačních studií a knihovnictví

DIPLOMOVÁ PRÁCE

Michaela Pappová

Analýza uživatelského chování vzhledem k ukládání digitální stopy bez vědomí uživatele

Analysis of user behavior due to the storing of digital footprints without knowledge of the user

Praha 2017

Vedoucí práce: Ing. Martin Souček, Ph.D.

Poděkování

Ráda bych tímto poděkovala vedoucímu absolventské práce, Ing. Martinu Součkovi, Ph.D., za trpělivost, veškerou pomoc, cenné rady, odborné vedení a připomínky při zpracování tématu. V neposlední řadě také děkuji všem respondentům, kteří mi poskytli potřebné informace a věnovali mi svůj čas.

Prohlašuji, že jsem diplomovou práci vypracoval/a samostatně, že jsem řádně citovala všechny použité prameny a literaturu a že práce nebyla využita v rámci jiného vysokoškolského studia či k získání jiného nebo stejného titulu.

V Praze dne 15.7.2017 podpis:…….

ABSTRAKT

Digitální stopa označuje data vzniklá při pohybu uživatele v digitálním prostředí nebo v interakci s ním. Vyskytuje se ve formě aktivní a pasivní, jež dohromady tvoří digitální identitu uživatele. Existující digitální stopa má pro uživatele největší přínos v personalizaci obsahu, se kterým přichází v digitálním i reálném prostředí do kontaktu. Slouží i pro utváření reputace uživatele na internetu. Pro další strany spočívá užití digitální stopy v marketingových a vědeckých účelech, užívá se i v personálních strategiích podniků či kriminalistice. Digitální stopy jsou omezitelné ze strany uživatele a existuje více strategií pro nakládání s digitální stopou.

Cílem této práce je analyzovat uživatelské chování studentů v digitálním prostředí a jejich znalosti o zanechávání digitální stopy. Zaměřuje se na vztah mezi uživatelskými znalostmi o existenci digitální stopy a reálným chováním online. Za účelem prozkoumání tématiky jsou stanoveny výzkumné otázky a posléze jsou zkoumány strategie uživatelského chování a nakládání s jejich údaji. Formou polostrukturovaného rozhovoru se zjišťují znalosti studentů o tématice digitální stopy a jejich chování online, s důrazem na motivace a důvody jejich nakládání s digitální stopou. Vztah mezi znalostmi a uživatelským chováním studentů je zjištěn, přičemž výrazně ovlivňuje strategii uživatelského chování na internetu.

Klíčová slova: digitální stopa, informační chování, uživatelské chování na internetu, studenti na internetu, bezpečné chování

ABSTRACT

Digital footprint designates data left behind a user movement in the digital environment or with the interaction with it. We distinguish active and passive digital footprint, which together creates a digital identity of the user. The biggest benefit of the digital footprint for a user is the personalization of internet content. It also creates the reputation of the user on the internet. For other parties its utilization comes in marketing and scientific purposes, it's also used in HR strategies of companies or criminology. Digital footprints are limitable from the side of the user and different strategies for managing it exists.

The aim of this thesis is to analyze user behavior of students in digital environment and their knowledge about digital footprints. It's focused on the relation between users knowledge about digital footprint existence and his real behavior. To fulfill the main purpose of the thesis researched questions are stated and afterwards the strategies of user behavior and managing their data are investigated. The knowledge of students and their real behavior with an accent on their motivation and reasons are determining in semi structured interviews. The relation between knowledge and real behavior was found out, whereas it influences the stratégy of user behavior online.

Keywords: digital footprint, digital trace, information behavior online, students on the internet, safe behavior

Obsah

Úvod

Digitální stopy jsou našimi otisky v digitálním prostředí – vyznačují naši cestu internetem jako šlépěje na zasněžené cestě, s tím rozdílem, že tyto digitální stopy na této digitální stezce již zůstanou, protože – použiji-li opět metaforu sněhu – sníh, který tvoří internet, netaje.

Digitální stopy vznikají při komunikaci uživatele skrze digitální média. Jedná se v surové podobě o data, nicméně v průběhu jejich zpracování jsou obohacena o kontext a vznikají tak z nich relevantní informace. Jako specifická forma informace jsou i digitální stopy předmětem studia informační vědy. Navíc zodpovědné nakládání s osobní digitální stopou je součástí informační gramotnosti, jíž by měli být vybaveni nejen vysokoškolští studenti[1]. Je však otázkou, do jaké míry si uživatelé doopravdy uvědomují, že zanechávají digitální stopu a zda, pokud si toho vědomi jsou, tyto znalosti ovlivňují jejich reálné uživatelské chování.

Tato práce si klade za cíl analyzovat uživatelské chování (tedy chování ve volném čase, mimo pracovní a školní povinnosti) vysokoškolských studentů na webu v závislosti znalostech o zanechávání digitální stopy. Nutným předpokladem pro úspěšnou analýzu je kvalitní zpracování tématiky digitálních stop a uživatelského chování. V teoretické části práce je tedy kriticky zkoumáno pozadí z teorie i praxe digitálních stop, které slouží jako vědomostní základ pro posouzení toho, co si respondent představuje pod digitální stopou a jakých aspektů ukládání digitální stopy si je vědom. Dále je v kapitole věnované informačnímu chování předložen vhled do přirozeného chování uživatelů na internetu, který shrne poznatky z literatury a výzkumů věnujících se této tématice.

Teoretickou část uzavírá krátký přehled odborných prací zabývajících se uživatelským chování na internetu a jeho propojením s digitální stopou. Jsou uvedeny výzkumy a kvalifikační práce z České republiky i zahraničí. V současné době neexistuje odpovídající výzkum, který by proběhl na území České republiky, tudíž byly vybrány výzkumy podobné svým zaměřením.

Hlavním cílem této práce je odpovědět si na dvě základní výzkumné otázky - “V jakém rozsahu si studenti uvědomují, že po sobě zanechávají na internetu digitální stopu?” a “Jaký dopad mají znalosti o digitální stopě na respondentovo uživatelské chování na internetu?” Za účelem odpovědí na výzkumné otázky proběhne kvalitativní výzkum popsaný v praktické části práce. Zde bude zkoumáno a analyzováno uživatelské chování na internetu na vybraném vzorku

[1] (Landová, 2002)

studentů pomocí polostrukturovaného rozhovoru, který nabízí určitou volnost pro reflexi přístupu respondenta k tématu a pro posouzení jeho reálného chování. Rozhovory se soustředí na uživatelskou úroveň respondenta, jeho znalosti problematiky digitální stopy, a především na jeho chování k digitální stopě.

1. Digitální stopa

Tato kapitola si klade za cíl vyložit teoretické pozadí týkající se digitální stopy, její využití, rizika a zákonná opatření na ochranu uživatelů v této oblasti. Představuje informace, na jejichž základě byla postavena struktura rozhovoru v klíčové části práce.

1.1. Uvedení pojmu

Žijeme v éře informačních technologií a systémů založených především na sítích. Rostoucí komunita uživatelů těchto technologií po sobě v digitálním prostředí zanechává rostoucí počet dat, a to cíleně svojí vlastní aktivní činnost či skrze senzory digitálních zařízení, která používají.

V současné době se dá říci, že digitální stopu po sobě zanecháváme skutečně všichni, ať už používáme počítač či nikoliv. Digitální stopa se totiž netýká jenom uživatelů informačních technologií, ale i běžného každodenního života jako je placení kartou či cesta do knihovny nebo restaurace. Nejznatelněji se však toto téma týká internetu, kde o sobě můžeme zanechat největší sumu informací. Digitální stopu po sobě uživatelé zanechávají buď vědomě, nebo nevědomě v různém spektru citlivosti. Leckdy nemají ani tušení, že i vědomě zanechané informace mohou být nějak použity či dokonce zneužity. Přičemž právě zanechání digitální stopy může mít vážné následky jako je krádež identity.

Studenti, se kterými jsem dělala na téma digitálních stop rozhovory, většinou přímo o termínu “digitální stopa” nikdy neslyšeli (samotný výzkum a jeho metodologie je popsán v kapitole č. 4) a v některých případech jej nebyli schopni ani odvodit. Jedná se však o ustálený termín spojený s počítačovou i informační vědou, forenzní vědou a kriminalistikou a především marketingem. Samozřejmě lze tento pojem v kontextu jiných vědních oborů vnímat zcela odlišně, a to např. jako digitální stopu hudby či jiného obsahu, řekněme tedy digitální nahrávku – cokoliv, co je v digitálním formátu. Pro přílišnou odlišnost významu se touto možností práce nezabývá.

1.2. Definice digitální stopy

Nejčastěji se digitální stopa definuje jako data zanechaná uživateli na digitálních službách či přístrojích (Arakerimath, 2015). Tony Fish (2009) definuje digitální stopu ještě trochu šířeji jako záznam interakcí s digitálním světem. K tomuto pojmu představuje však ještě nadstavbu - “moji digitální stopu”, jež obsahuje nejen uživatelova holá data či jejich metadata, ale i jejich analýzu a využití.

Snad původcem tohoto pojmu ve smyslu zanechaných dat v digitálním prostředí je John Battele (2004) ve svém zamyšlení nad vlastnictvím kolektivních dat nazvaném trefně „Z prchavého do věčného“, který se zde zmínil o digitální stopě[2] jako o vyčerpaném proudu kliků.

Od Batteleho pojem převzala americká společnost PEW Research Center ve svém výzkumu zaměřeném na management online identity (Madden a kol., 2007) a, přestože ještě v roce 2009 Garfinkel používal termínu “internetová stopa” (Garfinkel a kol., 2009), tak postupně vstoupil do všeobecného povědomí.

1.3. Formy digitální stopy

S dělením digitální stopy dle přičinění samotného uživatele do dvou kategorií – aktivní a pasivní – přišla jako první výše zmíněná společnost PEW Research. (Madden a kol., 2007) Pokročilí uživatelé si mohou být vědomi i zanechání pasivní digitální stopy, proto je dělení založeno i na tom, zda se uživatel může rozhodnout stopu nezanechávat. Tato klasifikace je obecně užívána, Tony Fish ji ještě doplňuje o kategorii vědomě nevědomou a přidává třídění dle tvůrce obsahu na digitální stopu tvořenou uživatelem, jinými uživateli a senzory. (Fish, 2009)

1.3.1. Aktivní

Aktivní digitální stopa je vytvářena uživatelem vědomě, dle jeho vlastní svobodné vůle a s vědomím vytváření určitého obsahu. Dle definice PEW se jedná o “osobní data zprostředkovaná samotným uživatelem skrz dobrovolné příspěvky či sdílení osobních dat” (PEW, 2007).

Aktivní digitální stopou tedy je obsah, který uživatel na internetu vytváří a uveřejňuje s vědomím, že tento obsah bude dostupný určitému obecenstvu, ne vždy si však plně uvědomuje šíři tohoto obecenstva.

Může se jednat o články, komentáře, příspěvky v diskuzních skupinách, uveřejněné fotografie či obrázky. Jedná se i o označení určitých položek (např. označováním zájmu na sociálních sítích - tzv. ”lajky” na Facebooku), profily vytvořené na sociálních sítích, e-shopech či jiných webových službách.

[2] „Our clickstream exhaust, so to speak.“ (Battele, 2004)

1.3.2. Pasivní

O pasivní digitální stopě oproti tomu nemusí vytvářející uživatel vůbec vědět. Jsou to data vznikající skrze čidla v jeho digitálním zařízení. Definice PEW praví, že pasivní digitální stopa jsou osobní data zpřístupněná bez záměrného úmyslu jedince (PEW 2007). I když si je uživatel třeba vědom toho, že stopu zanechává, nemůže tomu (při běžné uživatelské znalosti) zabránit.

Vytváření digitální stopy tedy není zjevné a uživatel je většinu času ponechán v nevědomí o tom, že vůbec nějakou tvoří. Proud informací jdoucí z uživatelova zařízení je takřka nepřerušený (Thatcher, 2014), dokud je uživatel připojen k internetové síti.

Tyto nevědomě zanechané stopy obsahují informace jako je fyzická adresa uživatele, čas přístupu k internetu, GPS polohu uživatele nebo oblasti jeho zájmu.

1.3.3. Vědomě nevědomá

Někdy se k těmto typům přidává i další druh digitální stopy, a to tzv. vědomě nevědomá. Jedná se především o obsah vytvořený jiným uživatelem, než kterého se týká. V takovémto případě uživatel leckdy ví, že obsah existuje, ale sám jej nevytvořil. Avšak vůbec to tušit nemusí, jedná se typicky o označené fotky na sociálních sítích, uveřejněné informace na webových stránkách škol či úřadů. Tento druh dat je většinou řazen do pasivní digitální stopy.

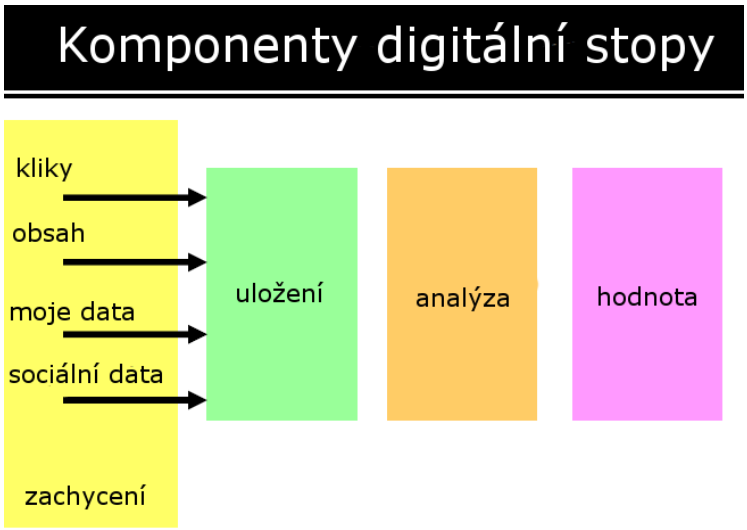
Digitální stopy vznikají jak aktivním vložením obsahu na internetu (tzv. aktivní digitální stopa), tak sledováním uživatelova chování (tzv. pasivní digitální stopa), na uživatelově digitální stopě se podílí i jiné osoby vkládáním obsahu o něm.

1.4. Komponenty digitální stopy

Digitální stopa je záznam uživatelovi interakce s mobilním přístrojem, webem, televizí, zkrátka čímkoliv, kde uživatel využívá internet. Avšak digitální stopy (především z té pasivní části) nejsou samotným uživatelům vůbec přístupné. Ač se tedy uživatel může zdánlivě jevit jako majitel svých dat, často neví a ani nemůže vědět, co je v rámci jeho digitální stopy uložené a v jakém rozsahu.

Tony Fish rozlišuje, co se týče komponent, klasickou digitální stopu jakožto syrová data a osobní digitální stopu (v originálu “my digital footprint”), již kromě syrových dat (viz

následující dvě kapitoly) tvoří i samotné uložení, analýza a hodnota digitální stopy jednotlivce viz obr. č. 1. (Fish, 2009)



Obrázek 1 Komponenty digitální stopy (Fish, 2009)

1.4.1.Rozsah digitální stopy

Digitální stopy různých uživatelů mají různý rozsah v závislosti na uživatelském chování. Obecně však platí, že se stále rozšiřují (je velmi obtížné odstranit z internetu něco, co tam bylo jednou uloženo). Data, ze kterých se sestávají digitální stopy, mají různé vstupy i výstupy. Výstupem těchto dat může být odhad uživatelova záměru – tedy předpovídá se jeho budoucí činnost na základě již zjištěných dat (podrobněji viz kapitola 1.5). Dále se hodnotí uživatelova reputace podle jeho zanechaného obsahu či tendence chovat se určitým způsobem. Celkově se snaží dané aplikace vytvořit o uživateli obraz, který by mohl sloužit k pozdějším účelům.

Podle společnosti EMC digitální prostředí každé dva roky zdvojnásobí svoji velikost a v roce 2020 bude již mít 40 ZB (EMC, 2014). Společnost EMC taktéž vydala kalkulátor digitální stopy, dle kterého si uživatel může vypočítat, kolik zhruba po něm zůstane množství dat. Pro osobu aktivní na sociálních sítích, e-mailu, sdílející obrázky a průměrně připojenou 10 hodin týdně (čas strávený průměrně na internetu dle dat ČSÚ pro skupinu lidí 16-24 let (ČSÚ, 2015a)), se jedná o 20 MB denně.

1.4.2.Aktivní uživatelova činnost

V rámci digitální stopy je sledován jakýkoliv obsah, který uživatel vytvoří, a jeho aktivita na internetu. Od příspěvku na sociální síti přes textový dokument po fotografii,

nahrávku či obrázek. Mezi data aktivně utvářená uživatelem patří např. osobní webové stránky, blogy, profily či příspěvky na sociálních sítích nebo jakýchkoliv jiných komunitních stránkách, obrázky i fotografie zveřejněné na internetových galeriích, fórech atd.

Aktivní digitální stopou jsou i e-maily, zprávy v chatu a zprávy vyměněné prostřednictvím zdánlivě soukromých konverzačních nástrojů instant messagingu či soukromé zprávy na messengerech typu Whatsapp nebo sociálních sítích. Bráno je tak i hodnocení různých produktů či služeb, komentáře v nákupních galeriích či jen nějaké rozpoznatelné označení produktu jako oblíbeného.

1.4.3.Pasivní činnost

Balíček aktivního obsahu vytvořeného uživatelem v rámci digitální stopy doplňuje řada metadat, která doprovází jeho aktivní obsah vložený na internet (na obr. č. 1 označeno jako "moje data"). Rovněž sem patří i data zaznamenávaná čidly na uživatelově zařízení. Jedná se o informace o poloze, druhu zařízení, fyzické adrese, typu a poskytovateli přístupu na internet atd.

Stezku uživatelova pohybu tvoří tzv. jeho kliky (popř. tapy, pokud se jedná o komunikaci s dotykovým displejem), které sledují jeho pohyb a chování v rámci aplikací či webových stránek. Sociální data obohacují digitální stopu konkrétního uživatele daty poskytnutými jinými uživateli. Jsou to textové zmínky, fotky, obrázky, hodnocení, reference, zkrátka informace aktivně poskytované internetu, akorát jinými uživateli.

Podstatnou část digitální stopy tvoří uživatelské chování obecně. Jde o informace o tom, jaké aplikace a služby uživatel využívá a skrze jaké zařízení do nich přistupuje. Zaznamenává se i časový průběh činnosti uživatele – jak dlouho v aplikaci či na webové stránce uživatel pracuje, co dělá (prohlíží obrázky, upravuje dokumenty, fotí…) a jak často. Tato data sbírá většinou nějaké příslušenství zařízení, nebo i přímo aplikace, kterou si uživatel cíleně nainstaloval (a většinou o sledovací funkci nevěděl).

Další datový záznam se vede o tom, kde se uživatel nachází. Sběr obsahuje vstupy získávané v reálném čase. Pokud jsou data uložena, poskytují informace o tom, kde se uživatel nacházel a jeho zvolenou trasu. Poloha bývá doplněna i o čas. Obecně se zaznamenávají informace o přesném čase i období.

Zaznamenávána je i uživatelova vyhledávací strategie a vyhledávání jako takové. Datový soubor poté tvoří řetězec požadavků na vyhledání a slova textu zadaná do vyhledávače. Vyhledávání však postupně stále více nabývá automatizované podoby na základě požadavků z

3D čárových kódů a informací dostupných v místě. Tyto informace jsou rovněž uloženy a doplněny časovou osou.

Digitální stopy neustále zvětšují svoji velikost. Čím více uživatel na internetu tráví času, čím více zařízení uživatel používá k přístupu, čím více se jeho život přesouvá do digitálního prostředí, tím větší jeho stopa je. Součástí jeho stopy je jeho aktivní činnost – osobní stránky, příspěvky na sociálních sítích, zprávy a hodnocení produktů či služeb, i pasivní činnost – údaje o jeho cestě internetem, otisk jeho zařízení, poloha, vyhledávání, čas akce a další podrobnosti.

1.5. Sběr dat a jejich využití

Účelem zaznamenání digitální stopy je zjednodušení uživatelova života – personalizace, jednodušší autentifikace a optimalizace služeb pro konkrétního uživatele. Slovy jednoho z respondentů je to to, "*k čemu to sloužit má*" (viz kapitola 4). Avšak primárně se digitální stopy využívají ke dvěma účelům – ke zkoumání uživatelského chování a k marketingu. Výzkum a reklama založená na digitálních stopách je stále na vzestupu, obzvlášť budoucnost marketingu spočívá ve využívání digitálních stop uživatelů.

1.5.1. Sběr dat

Existuje mnoho technologií mapující uživatelovo chování, sbírající o něm informace a ukládající je na různé servery jakékoliv strany[3]. Technologií s tímto nejvíce spojovanou jsou cookies, s nimiž běžní uživatelé přicházejí do denního kontaktu, avšak nejedná se o jedinou možnost.

Cookies

Cookie je krátký datový (textový) soubor, který server navštívené webové stránky odešle do prohlížeče. Prohlížeč jej dále uloží do počítače. Při další návštěvě stránky prohlížeč pošle soubor zpět serveru, který si z něj načte příslušná data. Cookies tak tvoří část uživatelovi digitální stopy, jež se ukládá přímo na jeho počítač.

Běžně si do cookies weby ukládají informace o uživateli, jeho předvolby, informace o návštěvě (strávený čas, počet prošlých stránek, nákup atd.) nebo i přihlašovací údaje. Při opakované návštěvě např. e-shopu již tedy uživatel nemusí znovu dávat do košíku položky,

[3] Strany osob na internetu jsou tři – první strana je navštěvovaná stránka/používaná aplikace ap., druhá strana je uživatel a třetí strana je jakákoliv jiná entita účastnící se kontaktu uživatele s používanou službou.

které do něj vložil předtím, vyplňovat přihlašovací údaje atd. Uživatelům je většinou přidělováno anonymní ID.

Dnes je mimo výše zmíněného účelu primárním cílem používání cookies odlišení jednotlivých uživatelů, zaznamenání jejich přítomnosti na stránce a zaznamenání zhlédnutí reklamy. Cookies mohou být vytvářena nejen stránkami, jež uživatel navštěvuje, ale také třetími stranami – především reklamními agenturami, které pak uživatele mohou identifikovat a sledovat na všech webech a vytvářet tak vzorce jeho chování a zájmů. (Sipior, 2009)

Společnost Google např. uvádí jako využití souborů cookies následující: "Používáme je například k ukládání vašich nastavení bezpečného vyhledávání, k výběru relevantních reklam, ke sledování počtu návštěvníků na stránce, k usnadnění registrace nových služeb a k ochraně vašich dat" (Google, cit. 2017d.).

Cookies mají určenou expirační dobu, tedy po určitém čase jsou z počítače samy odstraněny. Navíc jsou ukládány jako textové soubory a jsou tedy čitelné pro běžné uživatele.

Od roku 2015 je v České republice nutné vyžadovat souhlas s uložením cookies na základě nařízení Evropské unie. Příkaz k souhlasu s uložením cookies vydala i společnost Google pro všechny uživatele používající jejich reklamní systém či jiné služby. (Šablatura, 2015)

Local shared objects

Local shared objects jsou datové soubory, které mohou ukládat na uživatelův počítač weby používající Adobe Flash. Podle tohoto se jim někdy říká flash cookies, jelikož i funkci mají podobnou jako cookies. Odlišnosti jsou v tvůrci těchto objektů – tedy flash přehrávači a lokalizaci – méně dostupná lokalita v uživatelově počítači. Flash cookies nemají expirační lhůtu a jsou ukládána v binárním kódu.

Zombie cookies

Zombie cookies jsou cookies, která umožňují odlišným sledovacím prvkům sjednotit a propojit ID uživatelů přidělená skrze odlišné stránky nebo zařízení.

Pixelový tag

Pixelový tag, dále známý jako "web beacons" či pixelový GIF, je průhledný GIF nebo png soubor o velikosti jednoho pixelu umístěný v těle stránky. Typicky je používaný pro ověření zobrazení webové stránky či e-mailu. Po načtení pixelového tagu pošle prohlížeč

požadavek na server určení. Součástí požadavku je IP adresa, čas přístupu, druh prohlížeče a URL stránky. Také je možné skrze něj aktualizovat či vytvářet cookies. (Geary, 2012)

Tento typ sledovacího zařízení je nejčastěji využíván v e-mailech jako potvrzení přečtení či jiné akce se zaslanou zprávou nebo skrze reklamy umístěné na různých stránkách k potvrzení zobrazení reklam.

Fingerprinting

Další běžnou technologií pro sledování uživatelů je vytváření fingerprintu zařízení. Tento fingerprint představuje unikátní otisk počítače, mobilu atd. Skládá se z prvků, jako jsou fonty, typ procesoru, nainstalované doplňky nebo programy či připojené zařízení, a dohromady tvoří v některých případech až unikátní řetězec identifikující dané zařízení.

Dříve se fingerprint zanášel do souborů cookies, dnes je možné jej nahrávat především skrze HTML5 element "canvas" - plátno. Po načtení stránky je odeslán skript, který umožní "canvas fingerprinting" a instruuje počítač k nakreslení grafického prvku. Tento prvek je poté konvertován v token, který je možno sdílet mezi marketingovými společnostmi a docílit tak jedinečné identifikace uživatele.

Existuje více metod fingerprintu jako např. akustický, který vytváří identifikátor zvuku, který vydává konkrétní hardware zařízení při zpracovávání požadavku. (Kirk, 2014)

ID zařízení

U chytrých telefonů vzniká nutnost jiných sledovacích zařízení, vzhledem k tomu, že jejich uživatelé používají spíše aplikace než prohlížeče. V takových případech je sledováno ID zařízení, které uživatel používá. Princip funguje podobně jako fingerprinting počítače.

1.5.2. Využití digitálních stop

Široká škála sesbíraných dat identifikujících uživatele – jeho koníčky, zařízení, které využívá, chování online a leckdy i off-line, nabízí neméně široké využití. Nejzřejmějším je zpracování dat v marketingu za účelem různě cílené reklamy. Možná méně typická o to však důležitější je výzkumná činnost na poli digitálních stop a identit.

Leckdy si sami uživatelé neuvědomují, že digitální stopy mohou využít i oni sami a že jejich stopy mohou využít i jiné fyzické osoby. Z dalších běžných užití jmenujme využití ve forenzních vědách k sledování osob či shromažďování důkazního materiálu či personalistiku, kdy jsou digitální stopy užívány jako součást výběrového řízení či ke kontrole zaměstnance.

Věda, výzkum, monitoring

Díky své šíři a komplexnosti jsou digitální stopy, často ve formě nestrukturovaných velkoobjemových dat - tzv. big data, skvělým nástrojem pro výzkumy především sociálních či psychologických směrů. Sociální chování, osobní zkušenosti, predikce chování, výběr partnera, styl komunikace online – to je jen několik z témat výzkumů digitálních stop. (Golder, 2013) Výzkumníci dokáží lokalizovat uživatele s přesností na kilometry a posoudit osobnost člověka pouze na základě jeho profilu na sociální síti. (Youyou, 2015) Monitoring provádí nejen vědecké ale i státní organizace.

Vzhledem k šíři výzkumného užití bude prozkoumáno několik příkladů výzkumů v rešerši literatury v rámci další části této práce (viz kapitola č. 3)

Optimalizace

Využívání digitální stopy z hlediska první strany (tedy navštívené internetové stránky, používané aplikace atd.) bývá většinou pro účely či potřeby optimalizace nebo statistiky. Na základě informací, které daná strana o uživateli má, automaticky upraví svůj vzhled či obsah. Dále je možné uživateli doporučovat další nastavení nebo služby, jež tato strana nabízí. Mnohdy tato strana také sleduje uživatelův pohyb a v širším kontextu tvoří statistiky či analýzy pro zlepšování svých služeb nebo jejich lepší dostupnosti.

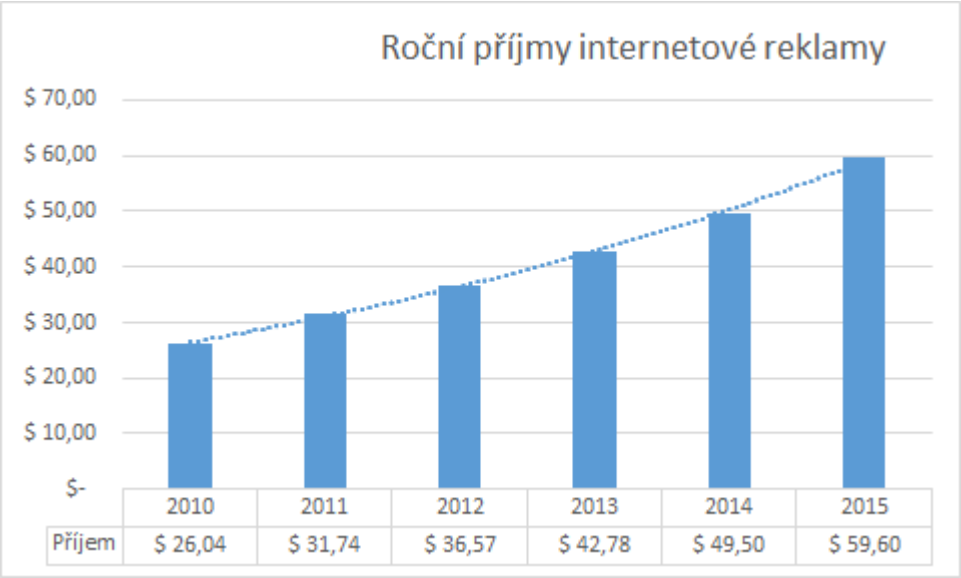
V zásadě z tohoto sběru informací profitují obě strany – uživatel má při opakované návštěvě k dispozici své nastavení a webová stránka má k dispozici přímou zpětnou vazbu od svých uživatelů.

Marketing

Data o uživatelích za marketingovými účely sbírají weby či aplikace (tzv. první strany) i externí marketingové společnosti (tzv. třetí strany). První strany mohou i nemusí sbírané informace předávat dál (záleží čistě na politice této strany a uživatel na ni je často upozorněn skrze vyskakovací okno a je nucen tuto politiku odsouhlasit).

Ať už se třetí strana dostane k uživatelově digitální stopě skrze svoje sběrné nástroje nebo je odkoupí od první strany, může je dále prodávat.

Většinový příjem dnešních poskytovatelů webových služeb je z reklamy. Příjmy z internetové reklamy neustále stabilně rostou (viz graf č. 1) a data jsou olejem online marketingu, navíc čím jsou rozmanitější, tím je jejich hodnota vyšší. 90 % příjmů služby Google je z webového marketingu, pro Facebook je to 95 %. (Liem, 2016)



Graf 1 Roční příjmy z internetové reklamy v USA

Hlavní význam digitální stopy z hlediska marketingu spočívá v ovlivnění zákazníka, především v udržení jeho loajality (Fish, 2009). Podrobné informace o uživatelově poloze, zájmech a chování mu umožní zobrazit patřičnou reklamu, která ho potenciálně zaujme, je cílená přesně na něj.

Cílená reklama se může rozdělit na tzv. retargeting a behaviorální targeting. Retargeting cílí na uživatele, který již někdy navštívil konkrétní stránku, přičemž mu je poté prostřednictvím reklamy na externích stránkách nabízen produkt, který si na první stránce prohlížel, a mohl by o něj tedy mít zájem. Behaviorální targeting využívá analýzy uživatelova chování na internetu, sleduje jeho vyhledávací činnost, lokalitu, návyky a navštěvované stránky v závislosti na rozsahu působiště reklamní agentury, která tato data sbírá. Z těchto sebraných dat je poté vytvářen uživatelský profil. Takovéto souhrnné informace – data s přidanou hodnotou – jsou z hlediska reklamy nejcennější, neboť umožňují nejefektivnější cílení reklamy.

Další využití

Ač se to nezdá, může zanechaná digitální stopa sloužit jako ochrana před zcizením uživatelových citlivých informací. Tento koncept se zakládá na tom, že uživatelé se chovají v rozpoznatelných vzorcích, které při porušení mohou znamenat, že se do uživatelova účtu či zařízení naboural někdo jiný. V takovém případě může být uživatel vyzván k ověření totožnosti skrze jiné kanály (např. e-mail).

Fingerprint daného zařízení stejně jako osobní digitální stopa bývá zcela unikátní, v kombinaci s uživatelským heslem tvoří téměř neprůstřelnou ochranu proti násilnému vniknutí do účtu. Tento styl identifikace uživatele používá např. společnost PayPal, která kombinuje

osobní údaje uživatele spolu s jeho IP adresou, otiskem prohlížeče a dalšími informacemi. (Liem, 2016)

Digitální stopa může v lecčem posloužit i uživateli samotnému. Uživatel si může tvořit statistiky o svém chování a vyvozovat z nich pak závěry pro své osobní účely. Mít rozpoznatelnou digitální stopu může také posloužit k sebepropagaci – tvorbě osobního brandu.

Podstatná část – především aktivní – digitální stopy je dostupná naprosto veřejně. Tuto část může volně využívat jakýkoliv uživatel internetu, který jakýmkoliv způsobem přišel k identifikátorům libovolného uživatele. Typickým příkladem jsou personální agentury či oddělení firem, jež si takto mohou zjistit informace o potencionálním zaměstnanci.

Ve specifických případech může digitální stopa posloužit i jako digitální důkaz a v takovém případě se může dostat do rukou státní správě, a to ať už v rámci policejního vyšetřování či v procesu správního řízení.

1.5.3.Rizika

Rizika digitální stopy se týkají především zneužití informací v ní obsažených. Uživatelé si leckdy neuvědomují, že všechny informace jsou zneužitelné, a i na první pohled důvěryhodné společnosti mohou jejich údaje prodat volně dál.

Obecně se dají rizika rozdělit na dvě hlavní kategorie, a to na ztrátu soukromí a na zneužití identity. (NCACIC, 2014) Zatímco odhalení soukromí může leckdy uživateli zkomplikovat život, zcizení identity jej může nenávratně poškodit.

Zneužití identity

Uživatelé během důvěřivého svěřování citlivých údajů jako jsou čísla kreditních karet, PIN kódy, hesla, rodná čísla atd. spoléhají na bezpečnostní protokoly aplikací, které však nejsou nikdy stoprocentní, a může dojít k úniku i takovýchto dat. (Salem Press Encyclopedia, 2016) Nejčastějším zneužitím za pomocí digitální stopy uživatele je krádež identity.

Krádež identity obsahuje zcizení osobních dokladů, ale také jakékoliv shromažďování a využívání cizích osobních i neosobních údajů, jejichž prostřednictvím se útočník vydává za jinou osobu, za účelem podvodu nebo jiné trestné činnosti. Většinou se jedná o obohacení. Krádež probíhá dvoustupňově – získáním údajů a poté jejich užitím.

V digitálním prostředí probíhá krádež získáním digitální identity, a to prostředky jako je neoprávněné kopírování dat, phishing[4] či přímo vniknutím do počítače (hacking). Na nejzákladnější úrovni se data dají získat i pomocí tzv. google hackingu – pouze pomocí internetového vyhledávače. (Krishnan, 2012)

Zneužití těchto údajů pak většinou bývá za účelem majetkového prospěchu, kdy se útočník za pomoci zcizených údajů může nabourat do bankovního konta. V některých případech se může jednat i o poškození dobré pověsti či práv, např. pokud se útočník naboura do cizího účtu na sociální síti nebo do e-mailové schránky a začne publikovat obsah jménem druhé osoby. Nejzávažnější forma krádeže identity je ta kriminální, kdy útočník zneužije cizí digitální identitu k trestnému činu. Setkáváme se i s krádeží identity za účelem vytvoření nové identity, kdy osoba převezme něčí údaje a na jejich základě si vystaví novou.

Zanechané informace mohou dále vést k riziku podvodných zpráv, které za pomoci dalších údajů z digitální stopy mohou být cíleně mířené i na konkrétní uživatele a o to se zdát důvěryhodnější. Zejména praktiky typu spam (nevyžádaná reklama), phishing[4] či spear phishing[5] mohou díky dalším doplňujícím informacím o uživateli působit důvěryhodněji.

Ztráta soukromí

Scott McNealy, generální ředitel Sun Microsystems, již roku 1999 řekl: "Nemáte žádné soukromí. Vyrovnejte se s tím." (Sprenger, 1999). Faktickým jevem, se kterým se každý den setkává každý uživatel internetu, je sledování a ukládání jeho digitální stopy.

Zanechané digitální stopy mohou mít vliv na uživatelův život z mnohých hledisek. Když vynecháme takové případy, kdy uživatele může na internetu snadno sledovat naprosto kdokoliv – ať už se to týká jeho zaměstnání, školy nebo civilního života – a tím posloužit jako problém v jeho soukromém či profesionálním životě – jakým způsobem toto omezuje uživatelovo soukromí?

Sledování uživatelů

Faktorem, který může řadě uživatelů přijít jako neoprávněné narušení jejich soukromí, je to, že většinu času jsou data sbíraná bez jejich přímého vědomí. (Arakerimath, 2015) V případě, že se společnosti podaří nashromáždit velké množství dat, může dojít k jednoznačné identifikaci osoby. Rovněž lze na základě těchto informací i provádět analýzy, jejichž

[4] Phishing označuje podvodné e-mailové zprávy tvářící se jako zprávy od důvěryhodného odesílatele snažící se vylákat důvěrné informace - např. číslo platební karty, hesla atd.

[5] Spear či cílený phishing – na rozdíl od phishingu se netváří jako známá služba, ale přímo jako známá osoba, kamarád či člen rodiny.

výsledkem můžou být i tak citlivé informace jako výše příjmu, rodinný stav, nemoci či movité vlastnictví.

I čistě se sledováním uživatelem skrze klasické cookies lze spojit určitá bezpečnostní rizika. Ta jsou poměrně nízká, týkají se však právě ohrožení ochrany soukromí. Navštívená stránka si totiž může do tohoto souboru ukládat zcela libovolné informace, jež o uživateli z prohlížeče zjistí. Většinou jsou pak tyto informace používány pro cílenou reklamu. Slabým článkem také může být samotný přenos od prohlížeče k serveru, který bývá napadnutelný. Navíc vzhledem k tomu, že webové stránky si do cookies často ukládají i přihlašovací údaje návštěvníků, je možné podstrčením patřičné cookie proniknout do uživatelova účtu bez skutečné znalosti těchto údajů.

Bohužel takto sbírané informace nejsou k dispozici pro uživatele samotné. Místo toho jsou uchovávány spolu s jejich analýzami v centralizovaných databázích reklamních agentur či velkých firem jako je Google, Apple nebo Facebook. (Sjöberg a kol., 2015). Uživatel tak nejenže nemůže tyto informace využít pro své účely, ale ani neví, co přesně o něm tyto společnosti všechno vědí.

Sběr uživatelských dat probíhá skrze objekty (jako jsou cookies či local shared objects) uložené přímo na uživatelově zařízení, ale i skrze objekty umístěné přímo v rámci aplikace či webové stránky (jako je pixelový tag či fingerprint zařízení). Takto sesbíraná data slouží k identifikaci uživatele, zaznamenání jeho chování či interakce s určitou službou. Dále se využívají v optimalizaci, vědě a výzkumu a marketingu. Ukládání těchto dat s sebou nese i rizika spojená s odevzdáním citlivých informací. Tyto informace mohou být zneužity již stranou, která je sbírá, mohou být dále prodány nebo mohou uniknout. Zneužitím v pravém slova smyslu je krádež identity, která může uživatele ohrozit na majetku či dobré pověsti. Dále s odevzdáním dat souvisí i jistá ztráta soukromí a cílené sledování uživatele.

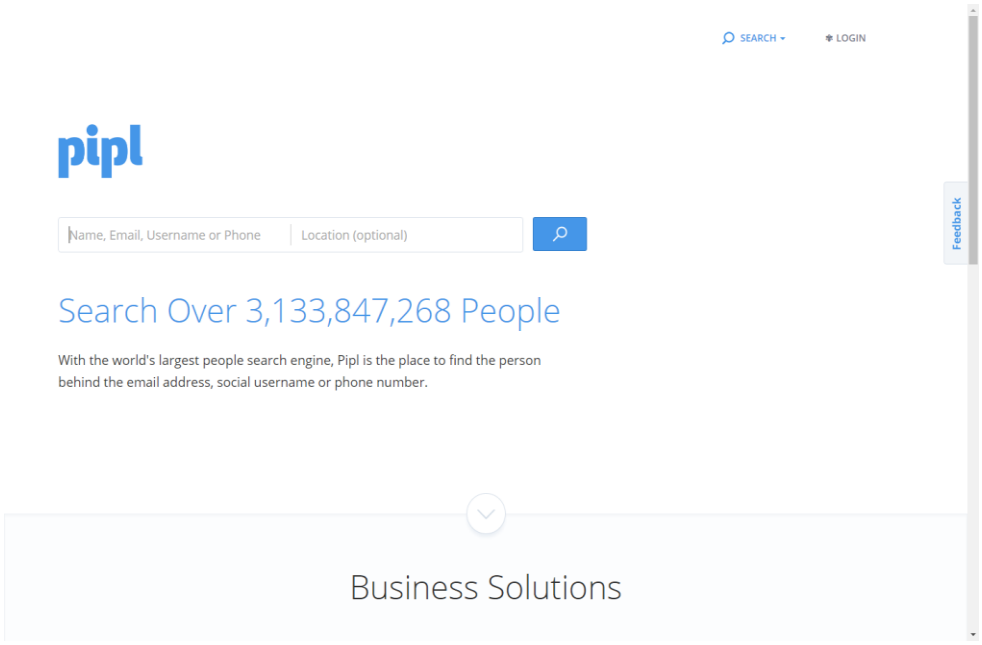
1.6. Možnost kontroly DS

Osobní digitální stopa je součástí každého individua, mají ji všichni uživatelé internetu a často i ti, kteří internet vůbec neužívají, jako kojenci, malé děti, mrtví lidé atd. Stačí, aby internet používalo jejich okolí. (Arakerimath, 2015) Mít proto představu o její podobě a vyhovující formu je v zájmu snad každého uživatele.

Již roku 2007 říká Ester Dyson ve zprávě PEW, že "uživatelé budou chtít podrobnější kontrolu nad jejich daty, dělat detailní rozhodnutí o tom, co je sdílené s kým a jak"[6] (PEW, 2007). Uživatelé v současné době mají určité možnosti pro kontrolu jejich digitální stopy.

1.6.1.Zjištění a kontrola

Prvním krokem pro úspěšný management digitální stopy a její kontrolu je znalost jejího rozsahu. Zjištění aktivní digitální stopy je ta jednodušší část, která probíhá především skrze egosurfing – vyhledávání sebe sama přes webové vyhledávače. Určité výsledky uživatel získá přes běžné vyhledávače typu Google, avšak pro podrobnější a detailnější výsledky je vhodné využít vyhledávače osob - tzv. "people search engines", které vyhledávají identity na základě identifikačních údajů jako je jméno, e-mailová adresa, telefonní číslo či lokace (viz obr. č. 2). Za pomoci těchto vyhledávačů je možné dát dohromady velmi důkladný profil veřejné digitální stopy.



Obrázek 2 Rozhraní vyhledávače pipl.com

Další možností důkladného zjištění rozsahu své digitální stopy je využít nástrojů používaných služeb. Např. Facebook nabízí stáhnutí veškerých informací o uživateli (pouze pro vlastníka účtu), v tomto souboru dat jsou mimo příspěvků a jiných informací běžně k nalezení na profilu zahrnuty i všechny aktivní relace, reklamy, na které uživatel klikl, tematické zařazení

[6] In the future, users are going to want more granular control over their data, making detailed decisions about what gets shared with whom. Users may be overwhelmed when first setting up an account, but when they get more comfortable with an application, they will exert more control. - Esther Dysoj (PEW, 2007)

reklam, IP adresy a další. Uživatel může v tomto souboru najít i data, která ze svého profilu smazal, odstraněné přátele, veškeré změny stavů a osobních informací, rovněž jsou k zjištění i data, která některé uživatele mohou překvapit, jako jsou údaje ze softwaru na rozpoznávání obličeje. (Facebook, cit. 2017)

Také společnost Google nabízí svým uživatelům podrobnou správu jejich dat. Skrze kartu Moje aktivita lze zobrazit každý krok, který uživatel udělal v jakékoliv aplikaci, kterou nabízí společnost Google. Pro uživatele prohlížeče Chrome nabízí i přehled jejich aktivity v tomto prohlížeči. Také tato data si může uživatel volně stáhnout v podobě archivu. (Google, cit. 2017a)

U pasivní digitální stopy sbírané především třetími stranami není její zjištění vůbec jednoduché, často je až nemožné. Výše zmíněná společnost Google nabízí kromě správy soukromí, také správu reklamy. V tomto profilu lze zjistit zaměření reklam a profil, který byl uživatel stvořen na základě buď jeho chování nebo informací, které přímo sdělil společnosti Google. (Google, cit. 2017b) Tyto informace lze nejen změnit, ale i nastavit, popř. zrušit zobrazování personalizované reklamy. Společnost Google četně uvádí, že "vaše osobní údaje nikdy nikomu neprodává".

Některé marketingové společnosti poskytují přístup do svých databází i uživatelům. Digital Advertising Alliance (DAA) je aliance sdružující reklamní společnosti, které nabízí uživatelům cílené reklamy obohacené o uživatelův interest. Myšlenkou těchto kampaní je ukazovat reklamu uživatelům, kteří o ni stojí, takovou, o jakou stojí. Např. společnost Acxiom umožňuje po ověření uživatelovi identity jeho přístup k nasbíraným datům. Bohužel pro české uživatele, jedná se z většiny případů o americké firmy cílící na americké uživatele. (Watson, 2014)

Určitý přehled o své digitální stopě si uživatel také může udělat skrze soubory cookies uložené na jeho počítači. Tato data ale nejsou uzpůsobena pro použití běžným uživatelem, proto je velmi obtížné se v nich orientovat.

1.6.2.Bezpečné chování

Základním předpokladem pro vyhnutí se potenciálním rizikům plynoucích ze vzniku digitální stopy je dodržování bezpečnostních zásad. Nutno dodat, že existují dva přístupy k udržení bezpečné digitální stopy: vytvoření jednotné jednoznačně identifikovatelné digitální identity založené na pravdivých informací a co nejvyšší anonymizace za pomocí využívání rozdílných účtů pod falešnými identitami.

Řada základních bezpečnostních pravidel, které uvádí společnosti jako je Cesnet, Google, PEW, je založena na zdravém rozumu a informační umírněnosti. (PEW, 2007), (Google, cit. 2017c), (Cesnet, 2014) Základními body vždy jsou:

- Bezpečné heslo a kvalitně zabezpečené účty skrze několika bodovou autentifikaci
- Bezpečné zařízení – užívání antivirového softwaru, aktualizované programy a operační systémy
- Užívání důvěryhodných sítí, popř. nesvěřování citlivých informací internetu při připojení skrze veřejné sítě
- Nastavení soukromí na svých účtech, nejen na sociálních sítích
- Kontrola komunikace – nekomunikovat s neznámými osobami, kontrolovat zabezpečení komunikace skrze certifikáty
- Opatrnost při sdílení citlivých dat
- Informační střídmost – neuveřejňovat citlivé informace
- Uvědomění si své neanonymity

1.6.3.Eliminace

Zanechání nulové digitální stopy se v dnešní době vylučuje s používáním informačních technologií. A i při naprosto nulovém kontaktu uživatele s digitálním prostředím, není jisté, že žádnou nebude mít – může ji za něj zanechat jakákoliv osoba, ať už blízká či třeba veřejná instituce jako úřad nebo škola.

Pro minimalizaci digitální stopy nejlépe slouží anonymní přistupování k síti. Základním nástrojem je internetový prohlížeč samotný. Nabízí prohlížení v anonymním režimu, ve kterém prohlížeč neukládá o uživateli žádná data, respektive je po ukončení prohlížení smaže. Naprostá nepropustnost však není zaručena a režim tak slouží především pro skrytí činnosti před případnými ostatními uživateli téhož zařízení.

Další funkce, kterou prohlížeče nabízí, je „Do not track“, jež do internetových stránek, které uživatel navštíví, vysílá požadavek na nesledování. Ne všechny stránky na toto reagují.

Do prohlížečů lze přidat i mnoho momentálně dostupných doplňků, které blokují sledování uživatele a ukládání cookies na jeho počítači. Mezi takové doplňky patří Ghostery nebo Privacy Badger. (NPR, 2016) Také fingerprinting počítače či prohlížeče lze blokovat

pomocí doplňků, jako jsou AdBlock Plus (doplněk primárně cílený na blokaci reklamy) či DoNotTrackMe. (Kirk, 2016)

Ještě efektivněji se uživatel může bránit za pomoci tzv. anonymizérů – programů či doplňků, jež mají za účel udržet uživatele v anonymitě, ať už před webovým serverem nebo různými nástroji pro sběr dat.

Anonymizéry mají různou podobu, nejčastěji ve formě proxy serverů – zařízení s přidělenou veřejnou IP adresou, které se bere jako prostředník mezi uživatele a cílovou webovou stránku (či její server). IP adresa uživatele je tedy překryta IP adresou proxy serevru.

Jednoduché proxy servery jsou běžně dostupné skrze klasickou webovou stránku s adresním řádkem, přes který se přistupuje na další stránky. Nejvyšší úroveň anonymizace nabízejí několikanásobné proxy servery – nástroje, jež směřují komunikaci mezi uživatelem a koncovým serverem mezi několika uzly. Tyto nástroje je již většinou nutné nainstalovat do uživatelova zařízení. Pak filtrují a upravují komunikace celého zařízení včetně nainstalovaných aplikací a informací, které tyto aplikace vysílají. Příkladem takovéhoto nástroje je Tor (The Onion Router). (Kříž, 2014)

Na podobném principu funguje připojení přes VPN (z anglického virtual private network, tedy virtuální privátní síť). VPN vytváří spoje sloužící pro přímé propojení uživatele se serverem, prostřednictvím kterého se uživatel připojuje ke všem službám dostupných na internetu. Tím pádem je jeho komunikace překrytá VPN serverem.

Pokud chce uživatel přistoupit k co nejvyšší míře anonymity na internetu a chce mít jistotu odstranění všech možných informací z prostoru online je velmi nepravděpodobné, že toto zvládne svépomocí. Tento cíl totiž obsahuje individuální kontaktování stránek s žádostí o odstranění informací o uživatelovi. Přičemž při registraci na službách typu Facebook, Google, LinkedIn uživatel dává přímý souhlas se zpracováním svých údajů a uděluje povolení k použití jeho informací. (Roček, 2012) V praxi to znamená, že pokud na Facebooku uveřejníte jakýkoliv příspěvek, nepatří vám, ale firmě Facebook.

Trh na zájem o co nejvyšší míru soukromí reaguje a vznikají četné společnosti jako Reputation.com, které pomáhají uživatelům monitorovat, odstraňovat či vylepšovat jejich digitální stopu. Tyto služby jsou většinou placené a orientované spíše na právnické či veřejné osoby. (Arakerimath, 2015)

1.6.4. Legislativa

Nedílnou součástí ochrany soukromí online je legislativní prostředí, především zákon č. 101/2000 Sb. o ochraně osobních údajů a o změně některých zákonů. Tento zákon je v souladu s předpisy Evropské unie a stanovuje podmínky, za kterých lze zpracovávat údaje vztahující se k jednomu člověku. Týká se veškerých osobních údajů zpracovávaných jakkoliv mimo osobní účely. Zákon určuje povinnosti správců informací uživatelů za účelem zabránění neoprávněného shromažďování, zveřejňování nebo jinému zneužívání. Mimo jiné definuje povinnost správce na vyžádání poskytnout žadateli informaci o zpracování osobních údajů.

Kontrolu dodržování tohoto zákona vykonává Úřad pro ochranu osobních údajů a jeho činnost je tímto zákonem vymezena.

Mobilní operátoři a poskytovatelé internetového připojení (a dalších několik stovek firem, které zákon 127/2005 Sb. o elektronických komunikacích definuje jako poskytovatele služeb elektronických komunikací) mají ze zákona povinnost uchovávat o každém uživateli po dobu šesti měsíců provozní a geolokační údaje. K těmto údajům může přistupovat pouze policie České republiky a další veřejné orgány s udělením souhlasu soudu a státního zástupce. Se svolením soudu lze rovněž nahlížet do obsahu sdělení různých messangerů či komunikátorů typu Whatsapp, Skype atd. (Rozmajzl, 2014)

Novinkou, která má teprve vejít v aktivní užívání, je Obecné nařízení o ochraně osobních údajů (General Data Protection Regulation neboli GDPR). Toto nařízení bylo přijato v dubnu 2016 Evropským parlamentem a vejde v platnost 25. 5. 2018. Bude se týkat shromažďování dat občanů Evropské unie, a to včetně institucí sídlících mimo území EU. GDPR zavádí pokuty za porušování stanovených pravidel a nařizuje větším zpracovatelům dat zřídit nezávislou kontrolní funkci úředníka pro kontrolu osobních údajů (Data Protection Office). Úkolem tohoto úředníka bude dohlížet na řádné zacházení s osobními daty a hlásit možné úniky dat či porušení zákona. (Škorničková, 2016)

Znalost rozsahu osobní digitální stopy je základem pro její kontrolu. Prvním krokem udělaným za tímto účelem by měl být ego searching – tedy vyhledání osobních údajů jako je jméno, telefonní číslo apod. na internetovém vyhledávači a vyhledávači osob. Dále kontrolou všech používaných služeb, přičemž firmy jako Facebook či Google nabízí svým uživatelům možnost stažení podrobného logu jeho aktivit. V případě eminentního zájmu je možné vyhledat služby specializované firmy. Dodržování zásad bezpečného chování (jako je opatrnost, informační střídmost, zabezpečení zařízení i účtů) je však primární pro udržení bezpečné

digitální stopy. V případě, že uživatel chce zamezit či významně omezit vznik jeho digitální stopy, nabízí se možnost využít anonymizačních prostředků, ať už přímo v rámci webového prohlížeče, různých anonymizérů. O bezpečnost uživatelských dat na internetu se stará i legislativa v podobě zákona o ochraně osobních údajů, zákon o elektronických komunikacích a budoucí evropské nařízení o ochraně osobních údajů.

1.7. Shrnutí

Digitální stopy jsou uživatelská data v digitálním prostředí, uživatel je aktivně tvoří publikováním obsahu, ale vznikají i zaznamenáním jeho chování a charakteristik jeho přístupu. Tato data se aktivně sbírají a používají k optimalizaci služeb, marketingu, vědě a výzkumu, může jich však využít i uživatel samotný – ať už svoji digitální stopu k sebeprezentaci nebo digitální stopy dalších uživatelů pro jejich dohledání či dohledání informací o nich. Kvůli tomuto sběru a možnosti identifikace unikátní digitální stopy je pro uživatele klíčové vědomí rozsahu jeho stopy a její kontrola, která je součástí bezpečného chování na internetu. O bezpečí digitálních stop se stará i legislativa, tak aby osobní informace byly zákonem chráněny.

2. Informační chování online

Uživatelé tráví na internetu čas z rozličných pohnutek a rozličným způsobem. Cílem této kapitoly je rozebrat a ilustrovat druhy informačního chování uživatelů internetu v jejich volném čase v závislosti na současné podobě digitálního prostředí. Za tímto účelem jsou popsány jevy, současné trendy a stav internetu, typologie uživatelů a jejich chování včetně vnímání jejich digitální identity. Závěr kapitoly je věnován českému prostředí za pomocí dat z Českého statistického úřadu.

2.1. Typy přirozeného informačního chování online

Internet je globální informační síť, informační prostředí, ve kterém uživatelé interagují pasivně či aktivně s velkým množstvím informací. (Erdelez, 1999) Umožnil nové formy lidské interakce a uživateli nabízí větší různorodost v chování. (Fisher, 2005) Informační chování na internetu se netýká pouze o vyhledávání informací, je i o jejich vytváření, sdílení a navazování sociálních vazeb.

Informační chování online pokrývá všechny aktivity, které uživatel dělá na webu. (Chun Yao, 2007) Tyto aktivity lze rozdělit dle toho, v jakém prostředí probíhají – v pracovním, formálním a neformálním – každodenním životě uživatele. V pracovním prostředí neprobíhá chování uživatele přirozeně, je zaměřeno na náplň jeho práce a má nízkou výpovědní hodnotu co se týče jeho přirozeného chování.

V širokém měřítku lze přirozené uživatelské chování rozdělit dle typologie Andrese Hektora (2003). **Vyhledávání a získávání** (search and retrieve) informací je typickou činností informačního chování. **Prohlížení** (browsing) neboli listováním více možnými zdroji. **Monitorování** (monitoring) je akt cíleného získávání informací opakovaným návratem či sledováním známého informačního zdroje. **Rozvíjení** (unfolding) označuje plynulé věnování se určitému zdroji – čtení knihy, poslouchání písničky, pouštění si videa. **Informační výměna** (information exchange) označuje odesílání a přijímání zpráv. **Komunikace** (nebo též oblékání – dress) pokrývá externalizovanou výměnu informací. **Pokynová aktivita** (instruct activity) spočívá v dávání pokynu, např. objednávka na internetovém obchodě. **Publikace** (publish activities) spočívá v extensivním zveřejněním informací.

Ačkoliv od roku 2003 internet změnil svoji podstatu, web přešel ze své podoby 1.0 do 2.0 a nyní se začíná mluvit o webu 3.0[7], tuto čtrnáct let starou typologie lze i dnes použít v praxi. Poslední dobou tak oblíbené osobní blogy lze zařadit do publikační činnosti, platby přes obchody s aplikacemi do pokynové aktivity, činnost na sociálních sítích do komunikace, chatování do výměny informací.

K chování uživatelů na internetu existují dva přístupy. První je založen na sociokognitivním pozorováním uživatelského chování v standardizovaném prostředí a druhý se zaměřuje na analýzu stop uživatelovi aktivity. (Lancieri, Durand, 2006) Chování na internetu v obecném hledisku za účelem vytváření typologií uživatelského chování, grafů a modelů bylo zkoumáno především z počátku 20. století. Od prvního zmíněného způsobu se upustilo a v současné době se téměř výlučně zkoumají data.

2.2. Web jako uživatelská platforma

Web jako statická veličina, na kterou by uživatelé měli pouze minimální vliv, je již minulostí. Na začátku 21. století se začaly projevovat principy webu 2.0. spolu se závislostí na uživatelské tvorbě obsahu. (O'Reilly, 2009) Uživatel je nyní jedním z klíčových prvků, které určují jeho podobu.

[7] Podstatou webu 1.0 bylo uživatelovo pasivní přijímání obsahu, který tvořil poměrně malý počet majitelů webových stránek. Web 2.0 je charakteristický aktivním zapojení uživatele do tvorby jeho obsahu, o době webu 2.0 se mluví cca od roku 2004. Web 3.0 ještě není pevně stanovený termín, se kterým se pojí především cloudové řešení běhu aplikací a ukládání dat, internet věcí (auta, spotřebiče aj. připojené k internetu) a sémantický web. (dále viz kapitola 2.2.1.)

2.2.1.Web 2.0

Tabulka 1 Vlastnosti webu 2.0 (O'Reilly, 2009)

Web 1.0		Web 2.0
DoubleClick	-->	Google AdSense
Ofoto	-->	Flickr
Akamai	-->	BitTorrent
mp3.com	-->	Napster
Britannica Online	-->	Wikipedia
personal websites	-->	blogging
evite	-->	upcoming.org and EVDB
domain name speculation	-->	search engine optimization
page views	-->	cost per click
screen scraping	-->	web services
publishing	-->	participation
content management systems	-->	wikis
directories (taxonomy)	-->	tagging ("folksonomy")
stickiness	-->	syndication

Statický web, nyní nazývaný 1.0 byl postupně obohacen o dynamičnost a přešel do vyšší vývojové fáze - 2.0. Základní myšlenou webu 2.0 dle jeho duchovního otce O'Reillyho je jeho použití jako platformy, respektive multiplatformy pro vývoj softwaru, dostupné pro kohokoliv, kdo má zájem se na vývoji webu podílet. Cílem vývoje webu by měl být bohatý uživatelský zážitek. Na jeho tvorbě by měli participovat i samotní uživatelé skrze nástroje, které jim budou volně dostupné – jako open source programy či API[8]. Tvorba obsahu webu se však zpřístupní jakémukoliv uživateli pomocí blogovacích nástrojů, wikipedie či wiki slovníky (viz tabulka č. 1). (O'Reilly, 2009)

Dalším důležitým prvkem webu 2.0 je tagování, tzv. folksonomie. Folksonomie opět souvisí se zapojením uživatelů do tvorby webu. Označuje tvorbu tagů – laických klíčových slov, které obsahu vymýšlí i přiřazují samotní uživatelé. Uživateli vytvořené tagy lze poté zobrazovat v tzv. tagových mračnech. (O'Reilly, 2009) Folksonomie je hojně využívána právě

[8] API – appliaction programming interface - je rozhraní pro programování aplikací, obsahuje sbírku procedur, funkcí, tříd či protokolů nějaké knihovny značně usnadňující tvorbu nových programů či jejich částí. Tvůrci programů často poskytují veřejné API pro použití dalšími osobami.

v blogovacích službách, ale i na sociálních sítích v podobě hashtagů, které může uživatel volně přiřazovat svým příspěvkům.

Rudman doplňuje technologické multiplatformní a komunitní faktory webu 2.0 o business procesy spočívající v cloudové technologii[9] a obecně v síťově dostupném softwaru a zdrojích. (Rudman, 2010)

2.2.2.Web 3.0

Web 3.0 je velmi složité definovat. Někteří jej udávají jako synonymum sémantického webu (Herman, 2009), jiní jako web dat (Williams, 2017) či jako internet věcí (internet of things) (Williams, 2017) Web 3.0 je možné pojmout i jako web virtuální reality. (Speicher, 2016) Obecně se tvrdí, že další vývojová fáze webu bude mít schopnost používat nestrukturované informace na webu inteligentně formulováním významu z jejich kontextu. (Verizon, 2015)

O webu 3.0 hovořil již Tim Berners Lee v roce 2001 (Berners-Lee, 2001), dosud však není v podstatě jasné ani to, zda už v jeho éře jsme či nikoliv. (Nations, 2017) Aspekty jako Internet of Things, sémantický web, virtuální realita či inteligentní agenti – programy schopné sbírat informace o uživatelích, zatímco se sami učí z jejich předchozích zkušeností, se již nyní začínají stávat běžnými součástmi webu. (Rudman, 2016)

Sémantický web

Sémantický web označuje web propojených dat. Data zde jsou strukturována a uložena podle určených pravidel a standardů. Toto uložení poté umožňuje jejich efektivnější nalezení. Sémantický web se především obrací k významu dat a až poté k jejich struktuře. (W3C, 2015)

Základem sémantického webu jsou tři technické standardy: RDF, SPARQL a OWL. RDF (Resource Description Format), jež je standardním rámcem pro popis a výměnu dat, popisuje informační zdroje pomocí výroků. RDF je běžně reprezentováno značkovacím jazykem XML.

SPARQL (Protocol and RDF Query Language) je sémantický dotazovací jazyk pro data uložená v RDF. Je speciálně navržen tak, aby dotazoval data napříč různými systémy.

[9] Cloudové technologie spočívají v poskytování služeb či programů servery dostupnými z internetu. Typicky se jedná o úložiště dat či software.

OWL (Web Ontology Language) je schématický jazyk sloužící k reprezentaci znalostí v rámci sémantického webu. Umožňuje definovat pojmy uspořadatelně tak, aby bylo co nejvíce možno je znovu použít. Každý pojem je tedy přesně definován. (Cambridge Semantics, 2017)

Internet věcí

Internet věcí nebo také objektů (Internet of Things nebo Internet of Objects) je koncept označující síťové propojení předmětů každodenního použití, které jsou vybaveny umělou inteligencí. Internet věcí rozšíří internetovou síť integrováním každého objektu, objekty budou komunikovat samy se sebou i s jejich uživateli. (Xia et al, 2012)

Koncept propojených zařízení pomocí internetu byl předestřen již Kevinem Ashtonem (1999) v roce 1999. Jeho ideou bylo, že kdybychom byli schopni sledovat a počítat vše, zabránilo by se plýtvání, snížily by se ztráty a konečná finanční nákladnost. V dnešní době díky poklesu ceny bezdrátových vysílačů a přijímačů a existenci protokolů, které mohou přiřadit miliardy různých adres různým zařízení, je již tento princip vykonáván. (Lopez Research, 2013) Senzory propojují živé i neživé objekty a sbírají velké množství dat.

Jako typický příklad aplikování internetu věcí lze jmenovat propojení telefonu s počítačem, ale možnosti jsou mnohem širší. Chytré aplikace dokáží být použity k monitorování jakékoliv lidské aktivity či k ovládání téměř libovolného spotřebiče. Integrované rozhraní, umožňující vzdálené ovládání a správu, může být zabudováno v autě, lednici, osvětlení či krbu. Chytré objekty dokáží i připomínat skrze náš telefon, že jsme si zapomněli vzít léky. Monitorování lidských biologických procesů také nikdy nebylo snazší – malému dítěti stačí připnout senzor, který rodičům na telefonu zobrazuje jeho teplotu, dech a další tělesné funkce. Takto lze monitorovat samozřejmě nejen malé dítě, ale i nemocné či jinak ohrožené uživatele. Propojená zařízení nabízí i sledování ztracených objektů a další a další možnosti využití v běžném životě. (Postscapes, 2017)

Hrozby webu 3.0 pro uživatele

Web 3.0 přináší kolaborativní a autonomní sbírání a zpracování uživatelských dat. Tato nová éra webu si sebou nese některá rizika ze svých předchozích etap a přidává některá další.

Sběr většího množství dat, které budou v době webu 3.0 naprosto klíčovým zdrojem informací, činí z bezpečnosti dat ještě více klíčovou otázkou k řešení. Neoprávněný přístup k důvěrným informacím provází celou historii internetu. Díky integraci a personalizační schopnosti technologií webu 3.0 však tento negativní dopad bude exponenciálně narůstat. (Bruwer, 2015)

Další negativní dopad související s jistým odevzdáním uživatelova soukromí do rukou inteligentních agentů a jiných aplikací je hyper cílený spam. Open sourcové založení webu 3.0 umožní spammerům lepší znalost anti spamového zařízení, množství potenciálně dostupných uživatelských dat umožní lepší cílení spamu a jiné nevyžádané pošty. (Rudman, 2015) Jako další zneužití uživatelských dat jmenujme již zmíněnou krádež identity (viz kapitola 1.5.3.). Pro získání uživatelských dat mohou útočníci využívat i slabin v dotazovacích jazycích, na kterých je web 3.0 postaven. Těmto útokům se říká SQL injection (popř. SPARQL injections) a spočívají v napadení databázové vrstvy programu skrze neošetřený vstup a vsunutí kódu – tedy vlastního škodlivého příkazu. (Bruwer, 2015)

Uživatel se čím dál tím více stává hlavním činitel webu, pro něj a kvůli němu se web vytváří a upravuje, avšak i sám uživatel se na jeho tvorbě čím dál tím více podílí a na toto je myšleno při tvorbě nové generace webu – tzv. webu 3.0, jehož éra je na spadnutí. S čím dál tím větším zapojením uživatele do tvorby webu pro něj vznikají i větší rizika spojená se ztrátou soukromí a důmyslnějšími metodami získávání a zneužívání dat.

2.3. Kolektivní inteligence na internetu

Princip kolektivní inteligence využívá zvýšené schopnosti kolektivů řešit problémy. Jedná se o univerzálně distribuovanou formu inteligence, konstantně zdokonalovanou, koordinovanou v reálném čase a vyúsťující v efektivní využití schopností všech (Lévy, 1997). Obecně je to proces týkající se velkých skupin individuí, které dávají dohromady svoje znalosti, data a schopnosti v rámci řešení problémů (Broadbent, Gallotti, 2015).

Internetovou síť tvoří kolektiv z uživatelů celého světa, kteří spolu navzájem interagují a kooperují pomocí sítí. Současně dochází k zachycení těchto sociálních dat, toků a komunikace a k pokusům o extrakci hodnoty z těchto dat. Uživatelé sítí jsou tedy zároveň producenti informací, znalostí a vztahů, tedy vytvářejí kolektivní inteligenci. (Bria, Primosig, 2013)

2.3.1. Využití kolektivní inteligence online

Jednou z nejdůležitějších funkcí webového prostoru je zachycovat a sklízet kolektivní inteligenci. Samotnou podstatou webu je propojení webových stránek skrze hyperlinky, akt, který by se jako takový dal nazvat aktem kolektivní inteligence, neboť uživatelé spojují jimi vytvořený obsah. (Surowiecki, 2014)

Li a Huang (2012) uvádí k ilustraci využití umělé inteligence sociální anotační systém a komunitní encyklopedii Wikipedia, jako příklad kooperativního tvoření znalosti. Podívejme se tedy na některá z využití kolektivní inteligence na internetu.

Sociální anotační systém

Sociální anotace označuje uživatelskou organizaci zdrojů. Kolektivní inteligence veřejnosti je využita k identifikaci a klasifikaci jakýchkoliv online zdrojů. Sociální anotace odráží znalosti jednotlivců, jejich zkušenosti, preference a návyky myšlení na odlišné informační rozložení, které ukazuje individuální kognitivní schopnosti účastníků. Tomuto druhu kolektivní inteligence se též říká sociální bookmarking.

Např. nástroj Delicious či Flickr umožňuje svým uživatelům ukládat webové stránky do záložek a opatřovat je štítky (tzv. tagy), při agregaci všech záložek a štítků je možno na jejich základě vytvořit (resp. uživatelé již vytvořili) reprezentativní schéma webu.

Na stejném principu uživatelské kolektivní inteligence funguje i vyhledávač firmy Google, jehož PageRank algoritmus reaguje na uživatelské prolinkování, uložení do záložek a jiné používání stránek.

Kooperativní tvorba a rozhodování

Internet rovněž pro své uživatele nabízí řadu dalších možnosti pro projevy kolektivní inteligence v podobě kooperativního tvoření nástroje, služby či znalosti. Tato tvorba většinou probíhá v komunitách, některé z nich mají hierarchické uspořádání, kdy nad obsahem utvořeným jinými uživateli dohlíží supervizoři. Příkladem hierarchické kooperativní komunity může být skupina lidí, kteří vytváří open source operační systém Linux, kde jsou uživateli vytvořené moduly pečlivě kontrolovány a vybírány týmem několika kontrolorů. (Malone, 2012)

Na otevřenějším principu, kdy se uživatelé kontrolují navzájem, funguje internetová encyklopedie Wikipedia, kde může kdokoliv vytvářet či upravovat jakékoliv články zcela svobodně. (Li, Huang, 2012)

Stejně jako vytvářet obsah uživatelé internetu i kolektivně rozhodují, jaký obsah vznikne, např. pomocí crowdfundingu, kdy uživatelé přispívají na vybraný projekt. Nebo rozhodují o tom, jaký obsah je kvalitní pomocí hodnotících či doporučovacích systémů jako je TripAdvisor (web s účelem doporučování výletních destinací, hotelů ap.).

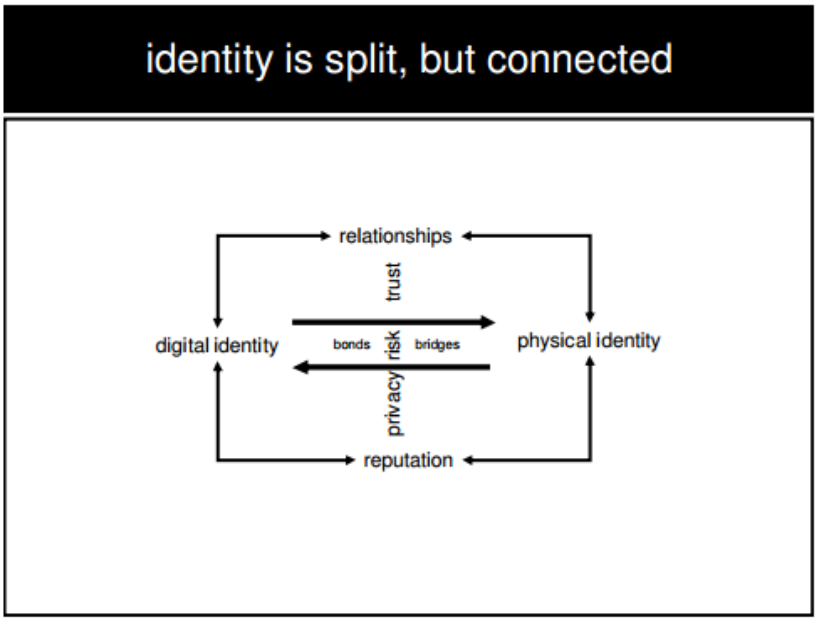
Principu kolektivní inteligence však využívají i komerční subjekty, kdy odměnou za uživatelem vytvořený obsah poskytují např. službu či produkt zdarma.

Nedílnou součástí současnosti a budoucnosti webu je uživatel a jeho inteligence, resp. inteligence kolektivní, tvořená velkými seskupeními uživatelů. Ve formě sociálních anotačních systémů (reprezentovaných sociálním bookmarkingem – správě a pořádání položek, např. záložek) a kooperativní tvorbě a rozhodování (na jehož základě vznikají četné stránky či služby shromažďující znalosti za pomocí početné komunity uživatelů – internetová encyklopedie Wikipedia, operační systém Linux, doporučovací systém TripAdvisor aj.).

2.4. Digitální identita

Identita značí v obecném měřítku totožnost, a to totožnost jedince. (Výrost, Slaměník, s. 109, 2008) Digitální identita nebo také internetová identita, online identita apod. označuje shrnutí digitálně dostupných dat o jednotlivci, nezávisle na jejich pravdivosti či veřejné dostupnosti. Obsahuje uživatelské charakteristiky a preference. (Liberty Global, 2012)

Digitální identita je propojená s tou fyzickou skrze různé mosty a pouta (viz obr. č. 3). Právě díky vlastnostem fyzické identity totiž ta digitální získává na hodnotě. Mosty jsou přímá spojení mezi identitami, např. platební karta, kterou jednotlivec používá jak k placení online tak off-line. Pouta označují společné klíčové znalosti či informace o obou. Tyto dvě identity jsou spojené i reputací skrze profily na sociálních sítích ap. (Fish, 2009)



Obrázek 3 Rozdělená identita (Fish, 2009)

2.4.1.Identita vs. persona

Digitální identita přináší svým uživatelům často pocit anonymity, který je do jisté míry dostupný skrze tzv. persony. Persona je projekcí určité osoby. (Maddox, 2014) Reálná osoba může i v běžném světě vystupovat pod více personami (např. spisovatel či herec s různými pseudonymy, ale i běžný člověk v rámci různých sociálních kruhů, ve kterých se představuje pod různou přezdívkou). Prostředí internetu ještě více usnadňuje tvorbu person. Uživatel může vystupovat pod herní přezdívkou na herním serveru a fórech, pod svým jménem a jinou přezdívkou na sociální síti a pod svým reálným jménem a příjmením např. v rámci svého zaměstnání.

Digitální persona je extenzí uživatele samotného, rozšiřuje jeho digitální identitu. Tyto digitální persony, které uživatel může všechny vést jiným směrem a může jich mít libovolné množství, jsou součástí jeho digitální identity. (Kerchkove, 2013)

2.4.2.Autentizovaná identita

Digitální identita slouží také jako osobní identifikace či autentifikace. Z hlediska bezpečnosti uživatelských dat je nutné co nejdůvěryhodněji propojit jeho digitální identitu a tu reálnou. (Kerchkove, 2013)

Autentifikace probíhá buď skrze něco, co uživatel zná, něco, co uživatel má, nebo něčím, čím uživatel je. Znalostí většinou bývá heslo, kdy uživatel sám potvrdí, že se skutečně

jedná o něj, jedná se o sebeověření. Majetkem bývá token, elektronický průkaz totožnosti vydávaný státem či certifikovanou autoritou – digitální podpis. Bytí označuje uživatelovy biometriky - např. otisky prstů. Pro vyšší spolehlivost ověření totožnosti je možné jednotlivé způsoby kombinovat. (Krhovják, Matyáš, 2007)

O jednotnou univerzální digitální identitu uživatelů se pokouší koncept správy identit třetí stranou, kdy má uživatel založen účet u důvěryhodného nezávislého poskytovatele, pomocí něhož se může přihlašovat i na partnerských službách. Příkladem takovéhoto systému je OpenID a na jeho standartu založená česká služba MojeID. Poskytovatel takovéto služby může po uživateli chtít i kombinované ověření totožnosti. Podobnou službu v současné době poskytují i sociální sítě či jiné webové stránky s velkým množstvím uživatelů, např. Facebook skrze službu Facebook Connect. (Guntovnikas, 2016)

Digitální identita uživatele je propojena s jeho reálnou identitou pomocí mostů, jako je jméno či platební karta. Digitální identita uživateli nabízí jistou míru anonymity skrze persony, projekce jedné identity, kdy uživatel může vystupovat s odlišnými identifikačními údaji na různých místech (někdy může působit i na stejném místě v rámci různých person). Pro přístup k citlivým účtům je proto nutné identitu autentifikovat, dokázat její propojení s tou reálnou.

2.5. Kategorizace uživatelů na internetu

Kategorizace uživatelů na internetu se zakládá na společném profilu různých skupin uživatelů. Tento profil je zakládán nejčastěji v závislosti na aktivitě uživatelů či na jejich důvěře v jejich bezpečí na internetu.

2.5.1. Na základě důvěry

Dr. Alan Westin se zabýval výzkumem vnímání soukromí uživatelů již od 70. let, během 90. let dále dal dohromady jednoduchou typologii osob v jejich vztahu k soukromí dat. Tuto typologii opakovaně testoval a měřil výskyt jednotlivých skupin v americké společnosti.

Fundamentalisté (Privacy Fundamentalist) je skupina, která vidí v soukromí velkou hodnotu, nikdy by svá data nevyměnila za službu a myslí si, že by to tak mělo vidět více osob. Bezstarostní (Privacy Unconcerned) dávají přednost benefitům a nevidí problém v poskytnutí svých dat vládě, autoritám či korporacím. Pragmatici (Privacy Pragmatist) zvažují poměr výhodnosti vydání jejich dat ke ztrátě jejich soukromí a chtějí vědět možná rizika. Dle měření

v roce 2003 je v americké veřejnosti 26 % fundamentalistů, 10 % bezstarostných a 64 % pragmatiků. (Kumaraguru, 2005)

Sheehan 2002

Sheehan (2002) ověřoval Westinovu typologii se zaměřením pouze na prostředí internetu. Dle jeho výsledků bylo fundamentalistů pouze 3 %, bezstarostných 16 % a 81 % pragmatiků.

Na základě svého výzkumu poté vypracoval pozměněnou typologii uživatelů internetu ve vztahu k jejich soukromí. Tyto skupiny jsou: bezstarostní (16 % uživatelů) s minimem obav o jejich soukromí online, obezřetní (38 % uživatelů) s nízkou obavou o jejich soukromí online, ostražití (43 % uživatelů) s mírnou obavou o jejich soukromí online a znepokojení (3 % uživatelů) s vysokou obavou o jejich soukromí online.

PEW 2007

Doplňme tuto Sheehanovu typologii závěry společnosti PEW, která se v roce 2007 zabývala důvěrou uživatelů v bezpečí jejich dat na internetu. Rozdělila uživatele do čtyř skupin na základě jejich důvěry.

Sebevědomí kreativci (Confident Creatives) představují skupinu uživatelů, kteří se nebojí o bezpečí svých dat a aktivně sdílejí svá data na internetu, avšak s určitou limitací osobních údajů. Toto je nejmenší skupina, která čítala 17 % Američanů.

Znepokojení a opatrní (Concerned and Careful) se o svá data strachují a aktivně se snaží o jejich limitaci. V této kategorii bylo 21 %.

Ustaraní na vedlejší koleji (Worried by the Wayside) se o svá data rovněž strachují, ale aktivně nelimitují informace, které o nich jsou dostupné online. Těchto uživatelů bylo 18 %.

Klidní a neaktivní se o svá data ani nebojí ani nelimitují informace, které o nich jsou dostupné online. Těchto byla největší skupina - 43 %. (PEW, 2007)

2.5.2. Na základě aktivity

Naprosto elementárním rozdělení uživatelů na základě jejich aktivity je model 1-9-90. Jak říká tento koncept, pouze minimum uživatelů - tzv. pracovníci – tvoří nějaký originální obsah (dle názvu modelu to může být 1 % uživatel), menšina - tzv. editoři – participuje v podobě občasné aktivity či komentování a sdílení a naprostá většina - tzv. okukovači – pouze sledují aktivitu ostatních a nikdy nebo velmi zřídka přispívají. (Jšnsson, 2014), (Goodier, 2012)

Dombrovskaya a kol. 2016

Širší typologii uživatelů internetu vzhledem k jejich aktivitám online v roce 2016 sestavila Dombrovskaya a kolektiv (Dombrovskaya et al., 2016). Tato typologie byla založena na základě mezinárodní analýzy a obsahovala pět typů: inovátory, charakterizované intenzivní konzumací jakéhokoliv internetového obsahu (12-16 hodin denně online), tradicionalisty, charakterizované nízkou konzumací internetového obsahu (1-2 hodiny online týdně), pobavené, kteří konzumují primárně rekreační internetový obsah poměrně intenzivně (8-12 hodin online denně), pragmatisty, konzumující převážně edukační a odborný internetový obsah (2-4 hodin denně online) a odpojené, kteří se do internetové komunikace z různých důvodů nezapojují.

Meyen a kol. 2010

Vzhledem k důležitosti a sociálnímu a kulturnímu kapitálu, který uživatelé získávají z internetu, vytvořil typologii tým Mnichovské univerzity (Meyen et al, 2010). Uživatelé jsou zde tříděni dvoustupňově – nejprve podle toho, jaký kapitál z internetu získávají (sociální či kulturní), a poté dle toho, jak pro ně je tento kapitál důležitý. (Viz tabulka č. 2)

Virtuozové (The Virtuosi) z internetu čerpají jak kulturní, tak sociální kapitál, který je pro ně velmi důležitý. Jedná se většinou o mladé, dobře situované a vzdělané lidi, kteří by se cítili ochuzeni, kdyby z nějakého důvodu nemohli, byť krátkodobě, být online

Profesionálové (The Professionals) využívají internet pro svoji práci, proto aby udrželi a rozvinuli své znalosti a dovednosti. Jedná se většinou o uživatele středního věku.

Závislí (The Addicts) jsou neustále online a hlavní kapitál čerpají ze sociálního rozměru internetu. Většinou si na internetu kompenzují nedostatek společnosti nebo osamělost v reálném životě. Jsou to většinou muži od mladého do středního věku.

Milovníci (The Aficionados) jsou k internetu připoutaní skrze jejich koníček či vášeň. Často se jedná o uživatele zralého věku.

Společníci (The Companions) svoje využití internetu směřují na sociální sítě, kde sbírají sociální kontakty a porovnávají se s ostatními. Internet pro ně není tak důležitý jako pro závislé, především kvůli dostatečnému sociálnímu kontaktu off-line.

Opatrní (The Cautious) používají internet pouze k základním úkonům typu nakupování a vyhledávání informací. Často nejsou schopni využívat internet na vyšší úrovní. Jedná se především o ženy středního až zralého věku.

Přidružení (The Affiliated) jsou online pouze za účelem udržení kontaktu s rodinou či známými. Používají internet ke své denní rutině, ale nic víc, není pro ně zásadní. Jedná se výhradně o ženy.

Tabulka 2 Typologie uživatelů internetu (Meyen et al, 2010)

TABLE 1
Typology of internet users

Relevance/capital	Cultural capital	Social capital
Very high	The Virtuosi	
High	The Professionals	The Addicts
Middle	The Aficionados	The Companions
Low	The Cautious	The Affiliated

2.5.3.Na základě přístupu k internetu

Jednou z nejvíce původních a nejpoužívanějších typologií uživatelů na internetu je ta Marca Prenskyho (2001). Dělí uživatele do dvou typů na základě jejich kompetence v užívání internetu. Prvním typem jsou digitální rodáci (Digital Natives), kteří se do doby internetu "narodili" a berou jej jako přirozené prostředí. V opozici k rodákům jsou digitální přistěhovalci (Digital Immigrants), jež se k užívání internetu dostali až v pozdějším věku a toto prostředí pro ně tedy není přirozené.

White a Le Cornu Prenskyho typologií upravují – základní dva typy dělí na obyvatele (Residents) a návštěvníky (Visitors). (White, Le Cornu, 2011) Návštěvníci vidí internet pouze jako nástroj či nástroje k dosahování určitých cílů. Používají sice internet, ale nepovažují se za jeho součást. Obyvatelé se na internetu "cítí jako doma", internet vnímají jako síť nástrojů i lidí a sebe vidí jako jeho součást. Tyto dva typy se prolínají, na jedné straně stojí totální obyvatelé a na druhé totální návštěvníci, avšak přechod mezi těmito typy není ostrý a uživatelé mohou mezi skupinami migrovat.

Mezi uživateli existují rozpoznatelné kategorie na základě jejich důvěry, aktivity a přístupu k internetu. Základní odlišností je to, jakou ve svém soukromí vidí uživatelé hodnotu, jak moc publikují unikátní obsah a jak jsou kompetentní k užívání internetu.

2.6. Čeští uživatelé na internetu

Dle informací Českého statistického úřadu za období 2016 (ČSÚ, 2016) má celkem 75,6 % českých domácností ve svém vlastnictví stolní nebo přenosný počítač, 18 % domácností má k dispozici chytrou televizi. 76,1 % českých domácností používá připojení k internetu. U domácností osob mladších než 40 let je to již 94,6 %. Naprostá většina (95 %) domácností s počítačem má tedy také přístup na internet.

50,9 % českých uživatelů se k internetu připojuje přes stolní počítač, 65,1 % přes notebook, 18, 4 % přes tablet a 53,9 % (uživatelů v kategorii 16-24 let je to 84,2 %) přes mobilní telefon.

77 % českých uživatelů se k internetu připojuje denně nebo téměř denně, přičemž 28 % na něm pro své soukromé účely tráví 1-5 hodin týdně, avšak 38 % mladých uživatelů do 24 let na něm tráví více než 20 hodin týdně.

2.6.1. Aktivity online

Čeští uživatelé ve svém volném čase využívají internet především ke komunikaci, dále pak k zábavě, vyhledávání informací a nakupování.

Elektronickou poštu využívá 94 % uživatelů a 54,1 % aktivně využívá sociální sítě (přičemž mladí uživatelé ve věku 16-24 let využívají sociální sítě z 94,9 %). 90 % uživatelů využívá internet k zábavě – čtení zpravodajských webů, přehrávání filmů nebo videí. Nejvíce uživatelé vyhledávají informace o zboží (89 %), poté cestování (62 %) a o zdraví (56 %). 61 % uživatelů na internetu nakupuje. (ČSÚ, 2016)

2.6.2. Obavy o bezpečnost

Celkem 4,6 % českých domácností, které nemají přístup k internetu tak činí kvůli obavám o své bezpečí či soukromí. 63,7 % uživatelů tvrdí, že rozumí pojmu cookies, ale jen 18,3 % ví, jak zakázat jejich ukládání. 67 % uživatelů někdy na internetu poskytlo nějaké osobní informace (jméno a příjmení, e-mail či telefon, číslo platební karty či fotky). 10 % uživatelů internetu omezilo v práci s internet bankingem kvůli obavám o bezpečnost, 10 % rovněž omezilo práci se sociálními sítěmi kvůli obavám o bezpečnost.

Dle výzkumu realizovaném agenturou Median (Median, 2017) na konci ledna 2017 se 49 % českých uživatelů internetu řadí mezi středně opatrné (používají několik bezpečnostních opatření k ochraně svých dat – středně silné heslo a antivirový program, dvoufázové ověření

totožnosti, atd.), 35 % k hodně opatrným (používají více bezpečnostních opatření) a 17 % k neopatrným (nepoužívají žádná bezpečnostní opatření a slabá hesla).

56 % uživatelů nepozná zabezpečené stránky, zbývajících 44 % (u respondentů do 29 let je to jen 38 %), kteří zabezpečení stránky rozpoznají, ji kontrolují alespoň občas. Obecně výzkum tvrdí, že mladá generace do 29 let podceňuje rizika, např. 95 % někdy umístilo na internet fotografii se svým obličejem. (Median, 2017), (Gordic, 2017)

Internet patří k ve většině českých domácností již k samozřejmosti, skrze něj se komunikuje, sdružuje na sociálních sítích, baví i nakupuje. Zejména využívaný je pak mladou generací. Obecně jsou na internetu čeští uživatelé spíše opatrní, avšak především mladá generace podceňuje rizika s internetem spojená.

2.7. Shrnutí

Přirozené informační chování na internetu spočívá v běžných aktivitách, které uživatelé dělají online ve svém volném čase. Web dnešní doby se stává platformou ideální právě pro toto chování, uživatelům nabízí čím dál tím více aktivit a uživatelé se rovněž podílí na jeho vzniku. Na internetu se podílí se na kvalitě jeho obsahu díky kolektivní inteligenci, vytváří si na něm digitální identity a persony a často jimi doplňují svoje reálné životy. Ne každý uživatel se však podílí na tvorbě webu ve stejné míře, stejně jako se liší důvěra v bezpečí jejich digitálních stop. Čeští uživatelé v tomto nejsou výjimkou, podle ČSÚ je polovina českých uživatelů středně opatrných a dalších 35 % hodně opatrných.

3. Rešerše odborných prací

Výzkum digitálních stop je v současné době oblíbené téma pojímané z různých úhlů. Tato kapitola má za cíl předestřít současný stav na poli výzkumu uživatelského chování na internetu s důrazem na kvalitativní metody výzkumu a vnímání zanechávání digitální stopy.

Je popsáno několik výzkumů zaměřených obecně na populaci a několik zaměřených na mladé uživatele, na které se zaměřuje i tato diplomová práce. Dále jsou uvedeny české i zahraniční klasifikační práce příbuzné tématikou i metodikou výzkumu.

3.1. Rešerše výzkumů

3.1.1. Self And Identity: Raising Undergraduate Students' Awareness Of Their Digital Footprints

Cílem skupiny výzkumníku Carmacho, Minelli a Grosseck (2012) ze Španělska bylo prozkoumat studentské vnímání jejich digitální identity, přístup k používání sociálních sítí a jejich opatření týkající se soukromí a šíření informací na internetu.

Výzkum byl prováděn na vzorku 135 studentů bakalářského studia katedry pedagogiky University Rovira a Virgili ve městě Tarragona ve Španělsku. Věkové rozpětí respondentů bylo 18 až 45 let.

Výzkum byl realizován pomocí facebookové aplikace The Museum Of Me, která slouží k sesbírání informací dostupných v jakékoliv formě na Facebooku včetně označení To se mi líbí různých zájmů či příspěvků přátel nebo propojení s jinými uživateli. Uživatel je v této aplikaci provázen virtuálním muzeem, kde jsou místo exponátů vystaveny jeho data z Facebooku.

Metodologie spočívala v dotazníkovém šetření před i po využití aplikace a skupinových diskuzích následujících každý dotazník. V části před použitím aplikace byly otázky soustřeďovány na druh informací sdílený online a na vnímání soukromí a bezpečnosti internetu. Po použití aplikace byly otázky zaměřeny na pocity vyvolané zhlédnutím jejich digitální identity a na odlišnosti a shody ve vykreslení.

Většina studentů je spokojená s vyobrazením jejich identity na Facebooku a zároveň si nedělá starosti s tím, jaké informace o nich mohou ostatní uživatelé vidět, protože přijímají opatření ke kontrole jejich činnosti online.

Samotní výzkumníci však konstatují, že výsledky nejsou reprezentativní pro celou skupinu studentů a doporučují další výzkum.

3.1.2. Digital Footprint (výzkumná větev)

Edinburská univerzita v čele s Dr. Connely (Connely, Osborne, 2015), (Connely, Osborně, 2015b), (Connely, Osborne, 2016) v letech 2014-2015 vedla výzkum s cílem detailního pochopení uživatelského nakládání studentů s jejich digitální stopou.

Výzkum poukazuje na to, že široce rozšířené přesvědčení o tom, že všichni mladí lidé jsou automaticky technicky zdatní, nemusí být platné. Na jeho počátku byla nejasnost rozsahu studentských znalostí vytváření digitální stopy a schopnosti její kontroly. Vzhledem k důležitosti digitální stopy v kontextu vyššího vzdělání byla seznána nutnost zjištění stavu a posléze vytvoření metodiky pro zaměstnance univerzity i jejich studenty ohledně vzdělávání v oblasti digitálních stop a bezpečného chování na internetu.

Východiskem výzkumu byla zvýšená míra studentského využívání sociálních sítí a podobných médií a výchozí předpoklad jejich nekritického používání a neinformovanosti.

Výzkum byl prováděn pomocí dotazníkového šetření ve dvou vlnách – v říjnu roku 2014 (587 respondentů) a květnu 2015 (870 respondentů), skupinových diskuzích se studenty, kteří předtím dostali za úkol v laboratoři zkoumat svou digitální stopu, a etnografickými rozhovory s šesti dobrovolníky (s nimiž proběhlo celkem 15 rozhovorů.

Z dotazníkových šetření mimo jiné vyplývá, že 61,6 % studentů nikdy nezměnilo nastavení soukromí na sociální síti, 5 % o sobě někdy našlo něco, o čem nevěděli, že je online, a 17 % uživatelů si je vědomo toho, že je o nich na internetu něco, co by nechtěli, aby ostatní viděli.

Celkovými závěry výzkumné větve jsou rozdílné přístupy studentů ve správě jejich identity a soukromí online. Ne vždy zvažují rizika prozrazení informací, které sdílejí ve zdánlivě soukromých aplikacích, jako jsou soukromé chaty či uzavřené profily na sociálních sítích. Většinou však studenti svoji digitální identitu formují tak, aby o nich vytvářela dobrý dojem.

3.1.3.Digital Footprints And Identities Community Attitudinal Research

Výzkum australského úřadu pro komunikaci a média (ACMA, 2013) zkoumal v letech 2012-2013 uživatelské pochopení a vnímání digitálních stop spolu s jejich managementem. Probíhal ve dvou fázích – kvalitativní ve formě online diskusních skupin rozdělených dle věku

a kvantitativní ve formě online dotazníků. Diskuzí se zúčastnilo 98 respondentů, dotazníky vyplnilo 2 509 respondentů.

Z výsledků výzkumu vyplývá, že si jsou uživatelé většinou vědomí zanechávání svých informací online, nedůvěřují v nastavení soukromí na různých stránkách a snaží se vyhnout riziku ztrapnění se či finanční ztráty kvůli úniku jejich citlivých informací. Většina uživatelů netušila, jak se digitální data sbírají a co se s nimi dá dělat, či jak se chovat, aby se uživatel potenciálnímu riziku vyhnul. Pouze každý desátý uživatel si pročítal obchodní podmínky, které přijímal.

Hlavním výsledkem výzkumu bylo vyvíjení rozličných identit uživatelů online – transakční, sociální a pracovní a jejich odlišná správa na základě různě vyhodnocených rizik pro každou identitu. Uživatelé kvůli komplikovanosti digitálního prostředí jen těžko sledují své vytvořené identity a ztrácejí o nich přehled.

3.2. Rešerše kvalifikačních prací

3.2.1. Nová média shromažďující informace o svém publiku a vztah uživatelů k bezpečnosti dat: kvalitativní studie

Davide Laube (2015) si klade ve své diplomové práci za cíl zjistit, jakým způsobem uživatelé vnímají své soukromí a bezpečí dat na internetu. Své výzkumné šetření vede pomocí polostrukturovaných rozhovorů se skupinou 10 respondentů, které dělí do dvou skupin – do 37 let a nad tuto věkovou hranici. Nutno podotknout, že nejmladšímu účastníkovi výzkumu bylo 27 let. K výzkumu byli voleni pouze uživatelé aktivní na sociálních sítích z okolí výzkumníka.

Rozhovory byly zaměřeny na čtyři témata: vztah k novým médiím, osobnost respondentů, způsob práce s novými médii a názory na to, jak nová média analyzují sebraná data.

Autor konstatuje, že mladší skupina uživatelů má o tématiku mnohem větší zájem a rozhovory s ní také trvaly déle. Rozdíl je také v aktivitě, kdy se starší ročníky hodnotí jako pasivně aktivní a mladší jako aktivní. Respondenti také tvrdili, že si jsou vědomi sledování online, především na sociálních sítích, avšak jejich představa o tom, v jaké míře toto sledování probíhá, se lišila.

U uživatelů obou věkových skupin byla identifikována souvislost mezi zájmem o téma a pocitem zásahu do soukromí využitím uživatelských dat. Uživatelům, kteří měli velký zájem o téma, vadilo použití jejich dat a vnímali to jako narušení soukromí. Uživatelé, kteří se

hodnotili jako běžní uživatelé bez velkého zájmu o tématiku, vnímali ztrátu soukromí jako podmínku používání internetu.

Výstupem výzkumu byly hypotézy o každé skupině uživatelů: "Uživatelé ve věku 26-37 let jsou na sociálních sítích aktivní a přemýšlejí o ochraně svého soukromí v kontextu svých činností." a "Uživatelé 55-67 let jsou na sociálních sítích spíše pasivní."

3.2.2. Young People and the Proprietary Ecology of Everyday Data

Ve své disertační práci G. T. Donovan (2013) předkládá mladé lidi jako kanárky v uhelném dole internetu, přirovnává je ke kyborgům, testerům, propojeným s digitálním světem, u nichž není jasná hranice mezi digitální identitou a tou skutečnou. Jsou to ti první, kteří vnímají změny v prostředí informačních technologií. Proprietární ekologie je prostředí uměle vytvořené mezi lidmi, médii a místy za účelem privatizace interakcí a různých dat stvořených těmito interakcemi. Mladí lidé dennodenně fungují v takovémto prostředí, kdy veškerá data, které produkují, jsou vlastněna třetí stranou a jen velmi vzácně je toto vlastnictví určeno i jim.

Cílem Donovana bylo prozkoumat, jak mladí lidé vnímají otázky identity, soukromí, vlastnictví a zároveň rozšířit povědomí mladých lidí o této tématice. K tomuto mu sloužily jako základ nestrukturované rozhovory s patnácti lidmi mezi 14 až 19 lety žijícími v New Yorku. Účastnící těchto rozhovorů si uvědomovali stinnou stránku digitální konektivity, ale neuměli ji identifikovat ani pojmenovat. Přiznávali závislost na hrách, Facebooku či počítači obecně.

Z rozhovorů vyplynulo pět dobrovolníků, se kterými Donovan v druhé fázi vytváří open source sociální síť, jejíž účel bylo navázat na témata rozhovorů a dále je rozvíjet. Soustředili se na demystifikace toho, jak je chování a zážitky online zaznamenávány. Za tímto účelem byli osloveni odborníci z digitální branže a byli požádáni o krátké video s vysvětlením tázané problematiky. Výstupem práce byla tedy sociální síť dávající dohromady základní body problematiky digitálních stop. Tato síť už bohužel v současné době není aktivní.

3.2.3. Analýza chování uživatelů sociální sítě Facebook

Tomáš Lehman (2014) ve své diplomové práci zužuje prostředí internetu na sociální sítě a sleduje chování jejich uživatelů pomocí dotazníkové šetření. Jako předpoklad k tomuto označuje sociální sítě jako nástroje ohrožující uživatelovo soukromí. Vzorek celkem dvě stě třiceti pěti uživatelů sociální sítě Facebook vyplnil dotazník zkoumající otázky uživatelské aktivity – především ochranu soukromí – a demografické údaje respondentů. Dále byla zjištěna

identita každého respondenta na Facebooku (vždy se jednalo o uživatele, které měl autor v přátelích) a byla provedena analýza obsahu sdíleného uživatelem.

Autor mimo jiné potvrdil své hypotézy: ženy vkládají na Facebook více fotografií než muži; uživatelé, kteří nečetli podmínky užívání Facebooku, publikují více příspěvků než ti, kteří je nečetli; existuje závislost mezi vzděláním a používáním her na Facebooku (čím nižší vzdělání, tím vyšší frekvence hraní her).

4. Sonda mezi studenty

Jak čeští studenti nakládají se svou digitální stopou na internetu a co si o této tématice myslí? Stejně jako ve výzkumu na Edinburské univerzitě (viz kapitola 3.1.2) se oprostíme od zažitých stereotypů toho, že jsou mladí lidé, obzvláště vysokoškolští studenti, technicky zdatní, zodpovědní a schopní managementu své digitální stopy. Cílem výzkumné části této práce je analyzovat uživatelské chování studentů na internetu v závislosti na jejich znalosti o ukládání digitální stopy a odpovědět si na základní výzkumné otázky.

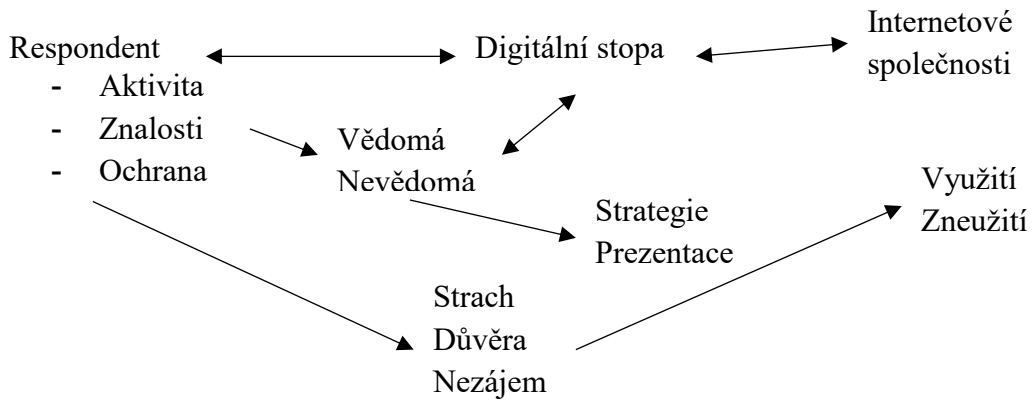
4.1. Předmět výzkumu

Předmětem výzkumu je uživatelské chování českých vysokoškolských studentů na internetu a jeho analýza v souvislosti s mírou jejich znalostí o vytváření a ukládání jejich digitální stopy.

Uživatelské chování z pohledu výzkumu označuje přirozené informační chování, jak je zmíněné v kapitole 2.1 – především publikace (tvorba obsahu), komunikace a výměna zpráv (chatování, sdružování se na sociálních sítích) a ochrana těchto dat.

Znalost v kontextu této práce označuje schopnost člověka uchovávat, komunikovat a zpracovávat informace. (Jonák, 2003) Nejde tedy jen o pasivní vědomí informace, ale její aktivní uvědomování.

Klíčovým je zjištění souvislostí mezi respondentovými znalostmi o ukládání digitální stopy, názory na soukromí na internetu a jeho reálném chování. Obrázek č. 4 znázorňuje konceptuální rámec zkoumané tématiky.



Obrázek 4 Konceptuální rámec výzkumu

4.1.1. Předpoklady výzkumu

Jediným předpokladem, na kterém stavěl tento výzkum, bylo aktivní využívání internetu mladými lidi. Dle ČSÚ (2016) jej totiž pravidelně používá 95,9 % lidí ve věku 16-24 let a 93,4 % osob ve věku 25-34 let.

4.1.2. Účel výzkumu

Účelem výzkumu je analýza uživatelského chování současných českých studentů v souvislosti s jejich znalostmi o ukládání digitální stopy na internetu. Cílem práce není zaujmout kritickou pozici, ale zcela otevřeně vysvětlit myšlení a jednání studentů spojené s jejich digitální stopou. Předpokládaným zjištěním je fakt, jak a do jaké míry ovlivňují aktivní znalosti ukládání digitální stopy uživatele jeho chování.

4.1.2.1. Výzkumné otázky

Pro snazší definici výzkumného problému bylo přistoupeno k rozdělení hlavního tématu a ke stanovení dvou hlavních výzkumných otázek spolu s doplňujícími otázkami sloužícími k upřesnění.

Otázka první: **V jakém rozsahu si studenti uvědomují, že po sobě zanechávají na internetu digitální stopu?**

Tato deskriptivní otázka má za cíl popis stavu znalostí o ukládání informací na internetu. Je doplněna dílčí otázkou: „Vědí, kdo všechno má přístup k jejich digitálním stopám?“

Otázka druhá: **Jaký dopad mají znalosti o digitální stopě na respondentovo uživatelské chování na internetu?**

Tato otázka je relační, ptá se, zda existuje vztah mezi znalostmi studenta o vytváření a ukládání digitální stopy a jeho chováním. Pokud tento vztah existuje, tak jaký.

Pro bližší upřesnění je otázka doplněna dvěma deskriptivními otázkami:

- „Jakým způsobem budují svoji digitální stopu?“
- „Jak (pokud vůbec) se snaží své digitální stopy chránit?“

Hlavním cílem výzkumu je odpovědět si na výzkumné otázky a dílčí otázky – analyzovat uživatelské chování studentů na webu v souvislosti s vytvářením digitální stopy. Dále je cílem předložit způsob přemýšlení studentů nad tématikou digitálních stop a s nimi souvisejícího soukromí na internetu a analyzovat jejich reálné chování na internetu.

4.1.3. Výběr vzorku kvalitativního výzkumu

Základním výzkumným vzorkem je celá populace vysokoškolských studentů. Na tento vzorek byla aplikována limitační pravidla pro omezení vlivu faktoru věku, základní vzorek tedy tvoří všichni vysokoškolští studenti do věku 26 let, studující na území České republiky.

Pro výběrový výzkumný vzorek, který by následně měl reprezentovat celou populaci studentů, byla zvolena kombinace dostupného a účelového výběru spolu s principem sněhové koule[10].

Bohužel bylo organizačně nemožné zajistit zcela náhodný vzorek. Aby se však co nejvíce omezil vliv blízkého okolí autorky a její subjektivní rozhodování, byli respondenti oslovováni skrze studentské fórum primat.cz a šířením v autorčině okolí s prosbou o kontakty na osoby ochotné rozhovor udělat. Rovněž někteří respondenti výzkumu doporučili další respondenty.

Při výběru vzorku byl kladen důraz na reprezentativnost a vyváženost vzorku z hlediska zaměření vzdělání, věku a pohlaví respondentů.

Nakonec výběrový výzkumný vzorek čítal patnáct studentů ve věku 20 až 25 let, pocházejících z vesnic, menších, středních i velkých měst a studujících převážně v Praze, také v Liberci, Ostravě či Olomouci široké spektrum oborů.

U patnáctého respondenta byl výběr ukončen, neboť rozhovory přestaly přinášet nová data či zjištění.

4.2. Metodologie

„Kvalitativní metody umožňují lépe porozumět sociálním vztahům a uchopit smysl, jenž lidé vlastnímu jednání i okolnímu světu dávají.“ (Hendl, 2005) Kvalitativní výzkum z principu nekvantifikuje data získaná od respondentů a umožňuje tak nejširší porozumění lidskému nebo sociálnímu problému. (Linderová, Scholz, Munduch, 2016) Kvalitativní výzkum je určený k vytváření nových zjištění, proto bude tato strana výzkumného spektra ideální k zjištění odpovědí na výzkumné otázky.

4.2.1. Polostrukturovaný rozhovor

Jako metodu jsem pro svůj výzkum zvolila polostrukturovaný rozhovor neboli rozhovor s návodem. Podstata takovéhoto rozhovoru spočívá ve vytvoření protokolu (viz příloha č. 1) se

[10] Princip sněhové koule označuje metodu, kdy stávající respondent doporučí další respondenty.

seznamem otázek či témat, které se během rozhovoru mohou klást v pozměněné formě, pořadí či je možné je doplnit dalšími otázkami dle uvážení výzkumníka. (Linderová, Scholz, Munduch, 2016)

Protokol byl nejdříve odladěn na předvýzkumu, který byl proveden se dvěma respondenty splňujícími pravidla konečného výběrového vzorku. Na základě těchto rozhovorů byly některé otázky rozhovoru přeformulovány, aby byly pro respondenty jasnější a srozumitelnější. Dále došlo ke zkrácení rozhovoru, neboť zkušební rozhovory trvaly více než 70 minut.

Struktura rozhovoru byla rozdělena do čtyř základních okruhů. Celkem bylo vytvořeno 24 povinných otázek doplněných pomocnými otázkami pro upřesnění odpovědi. První celek se zabýval sociodemografickými otázkami, jeho úkolem bylo nastolit atmosféru výzkumu a volně respondenta vpravit do tématiky.

Druhý celek zkoumal uživatelovu aktivitu na internetu, jeho běžné přirozené chování na internetu a strategii v publikování obsahu. Jednalo se především o deskriptivní otázky, volené tak, aby pro respondenta nebylo složité odpovědět.

V třetí části došlo ke zkoumání respondentových znalostí o zanechávání digitální stopy a obecně o této tématice včetně důvěry v bezpečnost a soukromí na internetu. V případě, že respondent neměl žádnou představu o zanechávání digitální stopy, byla mu pro umožnění pokračování rozhovoru přednesena definice: „Je to tvoje stopa v digitálním prostředí. Vytváříš ji aktivně ty i každý, kdo se o tobě zmíní. Vzniká však i bez tvého vědomí, skrz mobilní zařízení, aplikace či programy.“

Poslední celek měl za úkol zkoumat ovlivnění a motivace uživatelova reálného chování na internetu. Byl zaměřen na chování respondenta týkající se jeho soukromí a ochrany dat na internetu.

4.2.2. Průběh rozhovorů

Ke konání finálních rozhovorů bylo voleno neutrální či respondentem vybrané klidné prostředí, např. kavárna či studovna. Na začátku rozhovoru se výzkumník představil, nabídl respondentovi tykání a sdělil účel a téma rozhovoru. Respondent byl vzhledem k tomu, že se následně mělo jednat o jeho osobní či citlivé informace, se kterými je nutno zacházet dle pravidel etiky (WHO, 2011), ujištěn o naprosté anonymitě, přičemž k jeho další identifikaci bylo použito číslo. Dále byl respondent požádán o souhlas k nahrávání rozhovoru. Poté byla celá konverzace buď nahrávána, nebo byl pořízen přepis na notebooku. S nahráváním neudělili

souhlas dva respondenti. Nahrané rozhovory poté byly rovněž přepsány formou doslovné transkripce. (Viz příloha č. 2 na CD) Na konci byl rozhovor doplněn nabídkou na zaslání výsledků výzkumného šetření.

Otázky nebyly kladeny vždy ve shodném pořadí, některé byly i zcela vynechány. Např. z důvodu toho, že respondent samovolně žádanou informaci uvedl v rámci předchozí části rozhovoru, nebo se respondent nekvalifikoval pro odpověď na dotaz (typicky respondent, který neměl chytrý telefon, nebyl dotazován na věci podmíněné jeho vlastnictvím).

Délka rozhovorů se pohybovala mezi 31 až 55 minut, nejčastěji rozhovor trval mezi 37 až 45 minutami. Sbírání rozhovorů probíhalo od prosince 2016 do března 2017.

4.2.3. Limitace metody

Kvalitativní výzkum obnáší limitace ve formě relativně úzkého výběrového vzorku, kdy se tedy sesbírá velké množství informací o malém počtu jedinců. Lze tedy jen těžko výsledky výzkumu aplikovat na celou populaci a vytvořené hypotézy je vhodné ověřit např. kvantitativní metodou. (Disman, 2002).

Hrozbou konkrétně tohoto prováděného výzkumu je také málo náhodný výběrový výzkumný vzorek, který by mohl ovlivnit zobecnitelnost výsledků výzkumu.

Během rozhovorů mohlo dále dojít ke zkreslení ve formě „měření jako zdroj změny“, které spočívá v tom, že si respondent vytváří názor až na základě výzkumu. (Disman, 2002) Při rozhovorech se výzkumník často střetával s tím, že respondenti nad danou tématikou nikdy předtím nepřemýšleli a na některé otázky neměli zcela vytvořené názory.

4.3. Příprava dat

Odpovědi respondentů byly přepsány do záznamového archu v podobě komentované doslovné transkripce. Výjimku tvořili dva respondenti, kteří neudělili souhlas k nahrávání, u nich během rozhovoru došlo k opisu, avšak za účelem urychlení zápisu byl jazyk očištěn od chyb ve větné skladbě a byl drobně upraven stylisticky.

Analýza dat probíhala čistě manuálně vzhledem k rozsahu transkriptu pod sto stran, jež takovéto zpracování ještě umožňuje. Navíc tímto bylo docíleno bližšímu kontaktu s výzkumnými daty.

Odpovědi byly opatřeny značkami dle systému znaků W. Kallmeyera a F. Schütze (1976) pro zachování nonverbálních vyjadřovacích prostředků. Dále byly vytvořeny tři

kategorie: názory (znalosti), pocity, činnosti, na jejichž základě proběhlo základní kódování výpovědí respondentů. Tímto byly barevně odlišeny reálné činnosti (resp. reálné chování), názory (resp. znalosti) účastníků o tom, jak dochází k ukládání a užívání dat na internetu, a pocity a emoce s tímto spojené.

Pro činnosti byla zvolena oranžová barva, pocity fialová a názory modrá. Pro značení nápadných příznaků promluvy byly zvoleny následující značky: (‘) – zdvižení hlasu, tučný text – nápadné zdůraznění, (v) – váhání, (-) – kolísání hlasu, nerozhodný tón, (?) – tázací intonace, (..) – krátká pauza, (…) – delší pauza, (smích) – smích respondenta.

Např. „(')No jasně. Tak třeba na Instagramu šmíruju lidi, **to mě hrozně baví**.“

„Aplikaci fakt nemám. (...) Já jsem takovej (')asociál.“

„Anonymní režim nezapínám. To zapínaj (')ti, co jdou na porno. (smích) No, v podstatě to nepoužívám.“

4.4. Analýza dat

Za účelem adekvátního vyhodnocení a interpretace dat došlo k analýze dat pomocí dvojího kódování získaných rozhovorů. První kódování proběhlo za účelem vytvoření přehledné kontrastní tabulky pro kontrolu projektu a bylo úzce vázáno na výzkumné otázky. Druhé kódování, tzv. otevřené, proběhlo zcela nezávisle za účelem odhalení jevů a vystižení toho, co se v datech objevuje.

4.4.1. Tabulka pro kontrolu projektu

Tabulka pro kontrolu projektu je sestavována v rámci přípravy dat, ve fázi jejich redukce. Slouží k sumarizaci získaných dat, zároveň umožňuje komparační vhled a další využití v analýze a interpretaci dat. (Hendl, 2005)

Za účelem zodpovězení výzkumných otázek bylo přikročeno k vytvoření tzv. kontrastní tabulky pro kontrolu projektu, jež má za účel vytvořit přehledový nástroj k jasnému porovnání jednotlivých vlastností u skupin respondentů. (Miles, Huberman, 1994) Kontrastní tabulka (viz tab. č. 3) porovnává jednotlivé skupiny respondentů právě na základě jejich znalostí o ukládání digitální stopy.

Na základě konceptuálního rámce výzkumu (viz obr. č. 4) došlo k vytvoření pěti kategorií: znalosti, aktivita, důvěra, ochrana a zájem. Tyto kategorie byly dále škálovány na stupnici: žádné, minimální, průměrné, nadprůměrné, vysoké. Škály spočívaly v zachycení

trendu sledovaného u výběrového výzkumného vzorku, tedy se jednalo o relativní hodnoty označující, jaká je respondentova úroveň v porovnání s ostatními respondenty.

Data byla tedy kódována kategorií s její škálou. V textu byly vyhledávány jednotky (nejčastěji celé odpovědi na otázky), které prozrazovaly úroveň respondenta, a byly opatřeny patřičným kódem.

Např. uživatelčina odpověď na otázku „Vytváříš aktivně nějaký obsah na internetu?“ „*Mám blog, tak tam vytvářím obsah, teda když mám čas. Potom mám dokonce vařící videa na youtube. A jestli teda vkládání fotek na instagram je vytváření obsahu…, jestli se to tak dá brát. Tak určitě takhle.*“ byla vyhodnocena jako vysoká aktivita.

Odpověď na otázku „Co si myslíš, že je digitální stopa?“ *„Všechno. Všechny jako příspěvky, facebookový příspěvky, komentáře, všechny inzeráty třeba na tom vinted, no prostě, v podstatě všechno, co na tom internetu dělám víc, než že si něco přečtu, a v podstatě i to, že si něco přečtu je stopa, zaznamenávaná. To pak vidím v takových těch postranních reklamách, že tam mám samý šaty a nikdy tam nemám džíny, protože nakupuju jenom šaty. A tak podobně. Takže v podstatě všechno, co tam rozkliknu.“* A kdo ukládá tu digitální stopu? „*Nemám nejmenší tušení, se přiznám. Tak jako to tam prostě zůstane na těch serverech. Tomuhle já do hloubky moc nerozumím, se přiznám, to jsou všechno spíš nějaký moje dojmy, než spíš ověřený informace.“* Byla ohodnocena jako nadprůměrná znalost, neboť respondentka dala najevo vědomí toho, jakým způsobem její aktivní i pasivní digitální stopa vzniká, ale hned vzápětí dodává, že si odpovědí není jistá a tématice plně nerozumí.

Kategorie znalosti byla během kódování používána ve smyslu aktivního používání znalostí. Zpravidla, pokud měl uživatel vysoké znalosti, tak s nimi také pracoval, avšak k opačnému trendu docházelo u respondentů s nízkou nebo téměř žádnou znalostí. I tito respondenti, kteří nebyli schopni definovat pojem digitální stopa ani po navedení výzkumníka, poté v dalších fázích rozhovoru vykazovali jisté vědomí toho, že se jejich digitální stopa ukládá i pasivně. Tedy ač byli bez formálních znalostí, měli nějaké tušení. Kvůli těmto faktorům bylo nutno pročítat celý rozhovor k rozhodnutí o úrovni respondentových znalostí.

Tabulka 3 Kontrastní tabulka

Podmínky	Minimální znalosti (n=3)	Průměrné znalosti (n=4)	Nadprůměrné znalosti (n=4)	Vysoké znalosti (n=4)

Aktivita	Minimální *Většinou si to přečtu, ale nekomentuju.* *Nesdílím, spíš jenom komunikuju s těmi kamarády.*	Vysoké - 2x minimální - průměrné *Mám blog, instagram, youtube kanál...* *Nevytvářím. Jenom lajkuju věci.*	2x průměrné - 2x minimální *Jednou za čtvrt roku sdílím.* *Já tam moc informací nikde neudávám.*	2x Mírné - 2x nadprůměrné *Nic tam nedělám, nic tam nedávám.* *Snažím se prezentovat jako normální člověk.* *Jsou informace, který tam chci nechat, aby se ke mně lidi dostali.*
Důvěra	nadprůměrná - 2x minimální *Není důvod se hystericky obávat právě nějakého zneužívání.* *Nevěřit googlu hlavně...*	2 x průměrná x 2x minimální *V bezpečí nejsou nikde.* *Nemůžu říct, že bych tomu důvěřoval.*	Minimální - 3x průměrná *Žádný počítač není prostě v bezpečí.* *Věřím, že to používají. Ale ne proti mě.* *Otázka je, kdyby to uniklo, co se s tím stane.*	Průměrná *Já vím, že Facebook to přeprodává dál.* *Asi nějakým způsobem důvěřuju internetu, že je to v bezpečí.*
Ochrana	Mírná - 2x minimální *Většinou mám ty údaje stejné.* *Heslo mám všude stejný, abych ho nezapomněl.*	3x nadprůměrná - průměrná *Nechci někomu dát možnost mě ohrozit.* *Já už to víc zabezpečit asi nemůžu.* *Každé dva tři týdny vymažu historii a ty soubory cookies.*	nadprůměrná *Prevence je nejlepší.* *Snažím vždycky na každý účet si vymyslet jiné heslo.*	Nadprůměrná *Snažím se dávat věci, co nejsou zneužitelný.* *Mám komplikovaný a případně unikátní hesla.* *Zkouším ty aplikace.*
Zájem	Žádný - 2x minimální *Mě to nikdy nenapadlo.*	3x Mírný - adekvátní *Ani moc se o to nezajímám.* *Mně osobně to přijde důležité.*	2x průměrný - 2x nadprůměrný	Nadprůměrná *Nějaká forma zájmu by asi měla být u každýho.* *Člověk má mít povědomí, když něco dělá.*

4.4.2. Otevřené kódování dat

Ke kódování dat (viz ukázka kódování dat v tabulce č. 4) bylo použito tzv. otevřené kódování spočívající v rozdělení dat na jednotky a opatření jednotky patřičným kódem. Kódy byly vytvořeny na základě opakovaného čtení a samotného kódování dat. Jednalo se především o induktivní kódy, které dané výroky pouze nereprodukují, ale přidávají mu hodnotu. (Švaříček, Šeďová, 2007) Např. kód blog, který signalizoval, že má daný uživatel veřejný zájem spočívající v publikaci na internetu – tedy blog, účet na DeviantArtu, webové stránky atd. Kód nečtenář zase označoval uživatele, který o sobě prohlašuje, že nečte obchodní podmínky apod., které přijímá.

Tabulka 4 Ukázka kódování dat

25		Myslíš si, že informace, které jsi po sobě nějakým způsobem zanechal na internetu, jsou v bezpečí? - Když se registruješ např. na sociální síti, důvěřuješ, že data, která stránce svěříš, nezneužije? - Čteš si obecně obchodní podmínky? - Co bys ze zásady internetu nesvěřil? - Jaká rizika mohou plynout z tvé digitální stopy? Přijde ti celkově, že se na internetu chováš tak, že jsou tvá data v bezpečí? - V čem bys chtěl svoje chování změnit?	(')Ne. (smích) Tak.. já myslím, že tomu se dneska už nevyhneš. Jediná možnost je tam ten účet vůbec nemít, pak by z něj nemohli nic vytáhnout. (smích) Ne, to už by muselo bejt, abych si to přečetl. Jako nedal pro lidi, aby to viděli, nebo nezadal do nějakýho formuláře? Tak do formuláře to napsat musím, když si chci něco koupit. Ale tam tomu většinou věřím, když to po mně chce kreditku atd., tak tomu věřím, že se s tím nic nestane. A i kdyby jo, třak mám ještě na účtu autentifikace, že mi přijde smska, když mám něco zaplatit. Tak to mě až tak netrápí. Určitě bych někam nepověsil na fotce kreditku. Ještě z druhý strany třeba. Jako taky takový blázni jsou. Z mojí asi moc velký ne ale. (cmích) Myslím, že nic až tak kritickýho o mně po internetu neběhá. Leda tak moje návyky, co kam chodím a co tam dělám. To bych se musel zbláznit. No, snažím se. Teď jsem třeba nedávno upgradoval hesla na novou generaci, všude jiný. Na internetu? Tam asi v ničem. (smích) Nepřijdu si, že bych jako prolejzal nějaký...	nevyhnutelné nečtenář věřím připravený na zlo ostatní jsou nezodpovědní nic nebezpečného mnoho hesel snažím se sebedůvěra

Při tvorbě a kódování textu byl brán důraz na účel výzkumu, byly voleny kódy vztahující se k obecnému chování, popř. k jeho ilustraci. Ne však všechny jevy, ke kterým respondent udával informace, byly pro interpretaci dat důležité. Např. kódování využití konkrétních uživatelských aplikací v sekci zaměřené na uživatelské aktivity (otázky „K čemu využíváš internet?“ atd., viz příloha č. 1) bylo zaměřeno na obecné vzorce. Kód běžné tedy signalizoval naprosto standardního užívání, kterého se dopouštěla většina respondentů.

Byl vytvořen soupis kódů čítající v první fázi 122 kódů spolu s memy osvětlujícími jejich význam. U každého kódu bylo zaznamenáno, kde v záznamu rozhovoru se vyskytuje, v podobě kotvy.

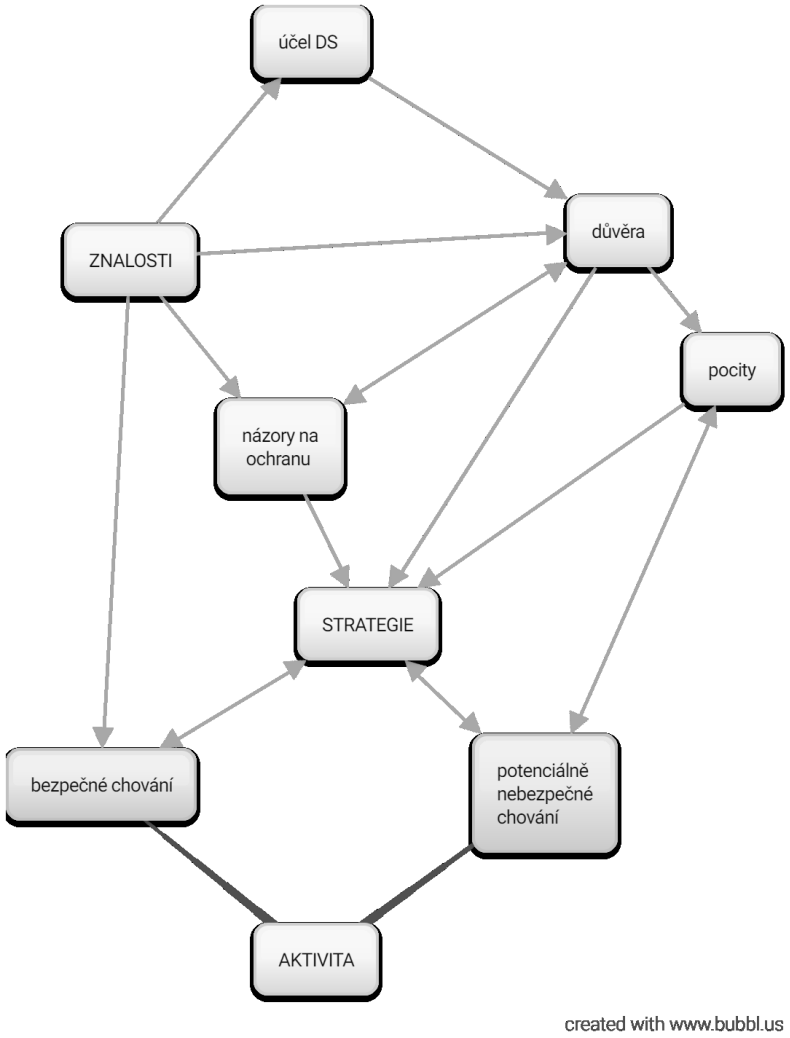
Tabulka 5 Ukázka soupisu kódů s memy a kotvami

cílená reklama	je si vědom vytváření cílené reklamy	F3-19;F5-18;F6-18;F7-16;F7-18;M9-18;F10-16;M11-18;M12-16;M13-18;M14-16;M14-18;M14-27;M15-16;F1-18;M2-18
vykrást	"když o sobě budu sdílet svoji adresu, tak mě může někdo vykrást"	M4-21;F8-26;F1-18
málo informací = bezpečí	bezpečí informací na internetu vidí v minimálním obsahu	F7-19;F10-19;M11-19;M12-19;M14-19;F1-19
silné heslo	zná zásady vytváření silného hesla	F3-20;M4-21;F6-19;F7-19;F8-21;F10-19;M11-19;M13-19;M14-19;M15-19;F1-19;M2-19
jedno heslo	používá pouze jedno heslo na všechny účty	F3-27;F5-12;F5-19;F5-23;F5-26;F6-12;F6-19;F6-28;F10-12;F10-23;M12-12;M12-26;F1-19;F1-26
reklama = zneužití	považuje použití informací v reklamě za zneužití	M13-19;F1-19

čtenář	čte obchodní či jiné podmínky, cookies, atd.	F8-27;M13-24
nečtenář	nečte obchodní či jiné podmínky, cookies, atd.	M4-25;F5-16;F5-26;F6-18;F6-25;M9-25;F10-16;F10-23;M11-23;M15-23;F1-19;F1-22;F1-23

4.4.3. Kategorie

V druhé fázi kódování dat bylo přistoupeno k vytvoření druhého setu kategorií závislém na otevřeném kódování. Kategorie tedy vycházely z kódů. Finálně se jednalo o tyto kategorie: aktivita, bezpečné chování, potenciálně nebezpečné chování, názory na ochranu, důvěra, vědomí, pocity, strategie, účel digitální stopy.



Graf 2 Kategorie se vztahy

Zjištěné kategorie byly v souladu (některé byly i totožné – znalosti a důvěra) s kategoriemi stanovenými v tabulce pro kontrolu projektu. Co však bylo unikátní, byly vztahy identifikované mezi těmito kategoriemi.

Díky definovaným vztahům vyšly jako klíčové kategorie aktivita, znalosti a strategie. Důležité v tomto schématu je, že v případě zkoumaného souboru nejen strategie vede k aktivitě, ale i naopak: tedy aktivita vede ke strategii, spolu se znalostmi o ukládání digitální stopy.

4.5. Interpretace dat

Během kódování a pročítání dat byly konstantně poznámkovány postupně se objevující jevy. Byly také zapsány poznámky vytvořené během samotných rozhovorů. Zapsané poznámky byly vzaty v potaz při interpretaci dat pouze v případě, že byly ověřeny na základě kódování či kontrastní tabulky.

Při interpretaci dat byly použity dvě metody analýzy kvalitativních dat. Metoda zachycení vzorců vyhledává a zaznamenává v datech opakující se vzorce, témata a struktury, byla zprostředkována využitím kategoriím vynořených z otevřeného kódování. Vzhledem k identifikaci odlišných vzorců chování studentů byla tato metoda doplněna metodou kontrastů a srovnávání, která od sebe odlišuje identifikované kategorie a nalézá mezi nimi rozdíly. (Švaříček, Šeďová, 2007)

Pro lepší orientaci v citacích od respondentů a zároveň zachování jejich anonymity byl každý student opatřen pseudonymem, jednoduchým českým křestním jménem. Zejména kvůli tomu, aby bylo možné spojit citace od stejného respondenta.

4.5.1. Analytický příběh

Jednoduchý popis kategorií a vztahů mezi nimi předkládá analytický příběh. (Švaříček, Šeďová, 2007) Grafické znázornění je možné vidět na grafu č. 3. Podrobněji budou zjištění předložena v následujících kapitolách.

Znalosti o zanechávání digitální stopy studentů jsou utvářeny jejich **pocity** a **názory** na ochranu dat založených spíše na zkušenostech sdílených se známými či získaných skrze média (např. kauzy ohledně úniků dat). Ze znalostí studentů vyplývá v přímé úměře **důvěra** v bezpečí jejich informací na internetu, kdy čím vyšší vědomí, tím vyšší důvěra, avšak pouze po dosažení průměrné míry. Znalosti o **účelu ukládání digitální stopy** rovněž ovlivňuje důvěru v přímé úměře, kdy čím více aspektů spojených s tímto jevem je studentu jasné, tím více důvěřuje.

Strategie uživatelského chování vyplývá ze samotných znalostí zprostředkovaných názory na ochranu jejich citlivých dat a důvěrou. Velký vliv na ni mají i pocity vyvolané důvěrou či nedůvěrou. **Aktivity** studentů týkající se ochrany dat mají dvě větve – **bezpečné** (nebo také zabezpečující), které vychází ze znalostí a strategie, a **potenciálně nebezpečné**,

konané na základě pocitů (především pocitu vlastní nedůležitosti) a zároveň vyvolávající pocity (především provinilosti či studu související s vědomím nebezpečnosti daného konání). Strategie ovlivňuje studentovy aktivity, kdy student volí chování podle jeho stanovené strategie (např. strategie nazvaná *připravený na zlo*, kdy student automaticky přepokládá maximální nebezpečí a podle toho jedná), ale i naopak jeho jednání ovlivňuje jeho strategii (např. pocit toho, že jeho data nikoho nezajímají, vyvolává buď absenci jakékoliv strategie, nebo strategii s nízkou ochranou).

4.5.2. Znalosti

Znalosti studentů o zanechávání digitální stopy se jevily klíčovým jak při sestavování samotného výzkumu, při kódování dat i při jejich interpretaci. Zkoumaný výběrový vzorek se skládal z jedinců, kdy si byl každý respondent v určité míře vědom ukládání digitální stopy.

Někteří respondenti (v kontrastní tabulce ohodnoceni úrovní znalostí jako minimální, viz tabulka č.3) si uvědomovali pouze ukládání jejich aktivní stopy a ukládání té pasivní nevnímali, nebo jen velmi okrajově, zprostředkovaně skrze zobrazení cílené reklamy. Při přímém dotazu na obsah jejich digitální stopy, respondentka Tereza uvedla: „*Cokoliv, co jsem kde napsala.“*, respondent Tomáš zase *„Tvoří ji určitě to, co přidám, fotky, komentáře, moje údaje, který někam zadávám, asi tak.“*

U této skupiny respondentů byl často rozpor, kdy si sami od sebe neuvědomovali, že se jejich chování ukládá (Tomáš v odpovědi na otázku, zda si uvědomuje, že jeho digitální stopa je tvořena i sledováním jeho chování: *„Jako... Že třeba si otevřu Facebook a koukám na příspěvky a jenom tím vzniká digitální stopa. (...) No, je to možný no. Nedivil bych se.“* Ale při spojení dotazu s reklamou, projevil pochopení této spojitosti: *„Já jsem se jednou podíval, že bych si koupil BMW, a teď mám všude reklamy na BMW. Nechtěj vědět, co se stalo, když jsem kupoval přítelkyni spodní prádlo.“*)

Ostatní respondenti si však byli vědomi zanechávání aktivní i pasivní stopy a tyto znalosti vykazovali v ohledu s jejich běžným uživatelským chováním. Tyto znalosti se lišily v hloubce poznatků o tom, jakým stylem se tato data ukládají, kdo je ukládá a co se s nimi děje.

Honza udává svůj obraz digitální stopy takto: „*Tak podle mého názoru je digitální stopa něco, co zanechává každý uživatel, co prostě surfuje po internetu. A všechny jeho aktivity se nějakým způsobem zaznamenávají, ať už do historie toho jeho prohlížeče anebo vyhledávače, tak jsou i soubory cookies… jsou přizpůsobené takové... Tak když jdeš na nějakou stránku, tak tam jsou ty soubory cookies.. A je to kvůli tomu, že oni shromažďují informace o tvém chování,*

ty se uloží do nějaké paměti a na základě toho ti například chodí reklamy, reklamy podle zájmu.“

Radek*:* „*Všechno. Cokoliv navštívíš, na cokoliv klikneš, kamkoliv se podíváš, pokud na to nemáš nějakej blok nebo TOR.*“

Helena: *„Všechny jako příspěvky, facebookový příspěvky, komentáře, všechny inzeráty třeba na tom vinted, no prostě, v podstatě všechno, co na tom internetu dělám víc, než že si něco přečtu, a v podstatě i to, že si něco přečtu je stopa, zaznamenávaná.“*

Typická představa respondentů na obsah jejich digitální stopy byl abstraktní pojem všeho, ačkoliv definice všeho se již pro každého respondenta lišila. Někdo považuje za součást své digitální stopy hesla jako třeba Aneta: „*Ale možná třeba i údaje tvoje, takový ty přihlašovací slova.*“, většinou však je vnímání digitální stopy jako každé akce na internetu. Alena říká: *„Každé kliknutí prostě na internetu*“,

Vědomí vlastní nevědomosti

Znalosti studentů o ukládání digitální stopy, především u těch s minimálním a průměrným vědomím, však vychází především z pocitů a názorů – přímo jejich nebo jejich okolí, z útržků informací, které někde zaslechli či přečetli.

Aneta se přiznává, že formálně o této tématice příliš neví, ale přijde jí, že to zná přirozeně: „*Tak jako ty poučky ne, ale tak to beru, že odjakživa tak ňák vim, že máš mít antivir a prostě pravidelně si tam nastavit ty kontroly a... A asi nic moc víc ne.*“

Lenka bere v potaz rady kamarádčina přítele Adama, který tomu dle ní rozumí lépe než ona: „*Tak jsem si říkala, že na tom asi něco bude, když Adam říká, že je to jako dobrý.*“

Helena se o toto téma nikdy příliš nezajímala, některé informace přijala během sledování večerního programu v televizi ze spotu Jak na Internet[11]: „*Tak před tím hlavním vysílacím časem běžel takovej tak tří minutovej spot o bezpečnosti na internetu. Tak na to jsem občas koukla, ale asi jinak ne*.“

Na druhou stranu si tato skupina respondentů vždy uvědomuje vlastní nevědomost a vyjadřuje až jisté pocity provinilosti či lítosti. Nejčastěji vyjádřené v ujišťování se o správnosti/nesprávnosti svých odpovědí.

[11] Televizní spoty Jak na internet mají asi dvě minuty, vycházely v letech 2012-2014 a stojí za nimi sdružení CZ.NIC ve spolupráci s Českou televizí.

Sára rozrušeně dává najevo, že je nepříjemné nevědět, co se s jejími daty na internetu děje a kde. „*No, ono to je dost hrozný, když o tom člověk nic moc neví, si myslim.*“

Tito respondenti často vyjadřují nevalné mínění o svých znalostech této tématiky jako např. Aneta: „*Docela v tom plavu, jak se mě ptáš. Přijde mi, že říkám hovadiny totální a pořád to samý dokola.“*

Znalosti jako takové jsou úzce spjaté s pocity studentů. Čím větší znalostní aparát o tom, co se s jeho digitální stopou děje, student má, tím slabší to v něm vyvolává emoce. Ačkoliv se výsledná strategie uživatelského chování neliší až tolik mezi studentem s vysokými a podprůměrnými znalostmi, pokud je podložena racionálními uvědomovanými informacemi, je mnohem klidnější. Radek téměř lakonicky dodává*: „Znalost bych asi měl, ale že bych na ni vždycky zas tak extra dbal, to zas ne. Ale tak jako vim, co bych měl dělat a tak.“*

4.5.3. Aktivita

Mezi respondenty se nacházeli studenti s širokým rozpětím aktivity na internetu. Od uživatelů, kteří deklarovali naprosto žádné cílené vytváření obsahu, resp. aktivitu omezenou na soukromou komunikaci s přáteli, po uživatele denně publikující na sociálních sítích či vedoucí si blog apod.

Radek říká o sociálních sítích: „*Většinou tam chodím, že se podívám a pak jdu zase pryč. Případně si s někým píšu, když tam někdo je*.“ Tímto dává jasně najevo účel, k jakému používá sociální sítě, a to spíše pasivní pozorování a interní chat s přáteli. Stejně tak se do dění aktivně nezapojuje Tereza: „*Aspoň poslední dva tři roky, řekněme, jsem na Facebooku skoro nic nepublikovala.*“ nebo Josef: „*Nic si nevedu, nikam nic nepíšu… Nejčastěji si píšu s lidma na FB a vyřizuju školní a pracovní maily.*“

Těchto uživatelů byla naprostá většina, v souladu s modelem 1-9-90 (viz kapitola 2.5.2.) by se dali nazvat jako „okukovači“, přičemž aktivita těchto studentů se omezuje právě na prohlížení obsahu vytvořeného jinými uživateli.

Jiný respondent Mirek rovněž jen pozoruje, a to obecně na celém internetu: „*Skoro tam ale nic nedělám, jen se koukám nebo třeba sleduju různý stránky.“* Aneta kromě sledování samotných příspěvků nebo článku čte i komentáře a reakce jiných lidí: „*Většinou si to přečtu, ale nekomentuju.“* Helena udává čtení komentářů jako zdroj zábavy: *„Vždycky ty komentáře jenom pročítám a... nevím, jestli se mám smát nebo brečet nad tím, jak jsou ty lidi blbí.“* Zájem o aktivitu jiných lidí projevuje i Lenka, která mimo jiné obsah sama i aktivně vytváří: „*Tak*

třeba na Instagramu šmíruju lidi, to mě hrozně baví, koukat jak někdo jinej žije, takový voyerství.“

O poznání menší skupinu tvořili uživatelé, tzv. editoři, kteří se do dění na internetu občas zapojí, ať už příspěvkem na sociální síti, diskuzním fóru či přispěním obrázku do veřejné galerie. U těchto editorů se jednalo téměř výlučně o sporadické zveřejňování příspěvků, které považovali za výjimečně zajímavé, na sociální sítě. Lenka: „*Tak na Instagramu ty fotky, když něco napíšu na tom vinted*[12]*, tak je to taky veřejný. (..) Občas něco sdílím na Facebooku, když mě něco fakt zaujme.*“ René: „*Používám DevianArt a podobné, takže tam nahrávám fotografie, uf... pokud se to dá považovat za vytváření obsahu. Také se dá samozřejmě považovat za vytváření obsahu každý příspěvek, který nahraju na FB*.“

Mezi respondenty byla jen jedna studentka, která se aktivně podílela na vytváření obsahu na internetu. Jako jediná měla aktivní blog, věnovala se vkládání příspěvků buď na něj, nebo na Youtube či sociální sítě. Dala by se tak klasifikovat jako pracovník tvořící pomyslné jedno procento aktivních uživatelů dle modelu 1-9-90. Sára: „*Mám blog, tak tam vytvářím obsah, teda když mám čas. Potom mám dokonce vařící videa na Youtube. A jestli teda vkládání fotek na Instagram je vytváření obsahu, jestli se to tak dá brát. Tak určitě takhle.“*

K nízké aktivitě studenty nevedou obavy o bezpečnost, spíše jako pocit, že nemají co říci, či alespoň ne nic zajímavého, popř. nemají potřebu se vyjadřovat. Tomáš (v odpověď na to, zda si vede blog): „*Přemejšlel jsem o tom, ale zjistil jsem, že by na to stejně nikdo nekoukal.*“ Tereza: „*Asi jako jsem radši..., když o sobě nesdílím všechno. (...) No, asi spíš jako kvůli tomu, že nemám úplně potřebu, to, že je to bezpečnější, je už jen takový bonus.*“

Tři další respondenti dokonce uvedli, že dříve mívali blog, avšak z nedostatku času či zájmu jej vést přestali. Jedna respondentka tento blog poté smazala kvůli obavě o citlivé informace umístěné na blogu, ostatní dva jsou stále dostupné na internetu.

Čtyři respondenti si pohrávali s myšlenkou, že by se chtěli na internetu prezentovat více, tvořit více obsahu, prezentovat svoje koníčky či zájmy jako třeba Radek, který vidí jako překážku nedostatečné vybavení: „*Tak eventuálně bych chtěl* [založit blog]*, ale musel bych mít lepší hardware. A nebo bych musel psát v angličtině*.“ Lenka zase vidí v aktivitě na internetu lepší šanci na pracovním trhu: „*Občas si teda říkám, že bych asi měla být aktivnější, vytvářet*

[12] Pozn. diskuzní fórum.

tam víc toho obsahu, abych měla víc šanci. Vytvářet si nějaký kredit na trhu práce, ale... Ještě mě to nijak zvlášť netrápí, když chodím do školy.“

Co se však týče bezpečného uživatelského chování, tak si jej studenti spojují opět s nízkou aktivitou. Základem je pro ně nesdílet potenciálně nebezpečné informace, ale pro dovedení k dokonalosti by bylo potřeba se vyhnout ukládání jakéhokoliv obsahu.

Tomáš: „*No, žádnou nevytvářet. Že bych nechodil na internet.*“

Štěpánka: „*Asi se vyvarovat... hm... těm mainstream stránkám jako je Facebook a vůbec těm stránkám, kde o sobě člověk sdílí strašně moc svých osobních dat. I proto si ho chci zrušit. Prostě se vyvarovat uveřejňováním svých dat. Člověk postuje svoji polohu, co kde kdy, v kolik hodin. To mi přijde jako nejvíc nebezpečný.*“

Mirek: „*Asi nebejt blbec, nesdílet všechno možný i nemožný někam, kde to každý vidí.*“

Sára: „*Vlastně nevím, jak to zabezpečit. Asi co nejmíň osobních informací dávat na internet.*“

René: „*Jedna věc je chovat se nějak zodpovědně na internetu a.... nesnažit se e... zbytečně o sobě uvolňovat informace, ale to je jen jakoby o množství dat nějaké v rámci té digitální stopy.*“

4.5.4. Strategie

Termínem strategie rozumíme především dlouhodobý záměr chování týkající se ochrany a bezpečí digitální stopy uživatele na internetu. Běžné uživatelské chování, jak bylo ilustrováno v sekci zabývající se aktivitou, je velmi konzistentní pro celý výběrový soubor, avšak má odlišné motivace, které poté ústí v chování strategicky zabezpečující či chování potenciálně nebezpečné.

Strategie studentů v udržování jejich digitální stopy se tedy liší a je závislá na více faktorech – znalostech (a názorech na bezpečnost), důvěře, vlastní aktivitě a pocitech. Přesto se dají najít vzorce určující strategii ochrany a aktivity na internetu. Rozdělme nyní respondenty na dvě skupiny dle tabulky pro kontrolu projektu – na respondenty s nadprůměrnými až vysokými znalostmi, kteří právě na těchto svých znalostech zakládají strategii svého chování, a skupinu s nižšími znalostmi, která své chování převážně zakládá na pocitech a názorech.

Strategie založená na znalostech

Respondenti s nadprůměrnými či vysokými znalostmi si jsou reálně vědomi toho, jak se mají chovat, aby udrželi svá data v co největším bezpečí, a dle tohoto vědomí se také chovají,

strategicky přistupují i k ochraně jejich dat zabezpečující strategií založenou na prevenci, protože jak říká Helena: „*Prevence je nejlepší*.“

Jednohlasně se shodují na tom, že primární je nesdílet citlivé údaje nebo je sdílet na stránkách/aplikacích s patřičným zabezpečením. Lenka říká: „ *No, přemýšlet asi v prvé řadě, co kde píšu. Co kde komentuju, co kde vkládám za fotky a za údaje.“* Hned poté k tomu dodává, že sama o sobě automaticky nic citlivého nezveřejňuje: *„A jinak nevim, nad tím jsem nikdy nepřemýšlela, já dělám na internetu tak nudný věci, že by to asi nikomu nestálo za to, aby to sledoval. A i kdyby, tak to není nic, za co bych se styděla nebo… bych to chtěla ochránit.“*

Avšak nesdílet citlivé údaje pro ně neznamená nesdílet vůbec. Odkazují na to, že tvorba obsahu není principiálně nebezpečná a ani sběr dat o chování člověka není primárně určen k jeho poškození. Michal je, co se týče jeho digitální stopy, v klidu: *„Zatím si říkám, dobře tak o mně někdo něco ví,“* dále odkazuje na to, že lidé na internetu sdílí jen ty informace, které by běžně sdělili i v normální konverzaci: *„ale rozdíl mezi věkem teď a kdysi je, že dřív za tebou mohl přijít nějakej agent, zeptat se tě a ty mu to u toho piva vyslepičíš, teď se může prostě kouknout na logy a stejně to ví. Tak jako je to to samý, jenom za tebou nemusí chodit. To je jako všecko. Tak jako když dělám věci, který mi jsou jedno, jestli je proti mně někdo použije. Cokoliv uděláme na internetu, tak někdo může použít proti nám, tak jako ok.*“ Dokonce je pro něj žádoucí, aby byl jako konkrétní osoba dohledatelný: „*Určitě jsou informace, který tam chci nechat, aby se ke mně lidi dostali. l třeba až budu psát nějaký vědecký články. Jak mě kontaktovat a tak. To chceš, aby tě lidi našli.*“ René zase publikuje vybrané příspěvky na Facebooku veřejně, aby mohl každý vidět, co mu přijde zajímavé: „*Protože mám pocit, zas když tam někdo vleze, tak mám pocit… to je hezké, reprezentativní, to všichni uvidí, jak jsem šikovný*.“ Mirek aktivně participuje na vylepšování map firmy Google: „*Jako já to mám v principu otevřený dost, píšu i recenze v Google local guides, a to se zobrazuje komukoliv*.“

V rámci strategie na zajištění bezpečí svým digitálním stopám však tito respondenti postupují také kroky v podobě nejen pasivní znalosti ale i reálného dodržování zásad bezpečného chování (viz kapitola 1.6.2.) zprostředkovaného skrze kontrolu zabezpečení stránek, žádoucí nastavení soukromí, ego searching za účelem zjištění dostupnosti informací o nich a dodržování silných hesel. Mirek si uvědomuje, co o něm je na internetu dostupné: „*Občas se googlím, jestli se to dá počítat. Jdou na mě najít nějaký veřejně viditelný fotky spojitelný s mou osobou...“* A hned zdůrazňuje: *„Nic špatnýho jako.*“ (…) „*No, tak zajímá mě to, co o mně je na internetu. Když si představím, že si mě vyhledává nějakej personalista.*“ René říká v nadsázce: „*Googlil jsem se už v minulosti. Přiznávám se k tomuto aktu. É... Moc toho není,*

momentálně se o mně dá zjisti, že jsem na Facebooku, Twitteru a že jsem někdy nafotil nějakou fotku. Přinejmenším při běžném hledání přes Google.“ Helena zase ví, že primární obsah, který je o ní veřejně dostupný, nepublikovala ona: „*A co k mýmu jménu vypadlo, byly samý výsledkový listiny olympiád, různých jako středoškolských soutěží a podobně.*“ René hlídá zabezpečení stránek před přihlášením: „*Kontroluju, jestli tam je SSL certifikát. Jestli to běží na https.*“ Michal omezuje přístup nainstalovaným aplikacím: „*K nejmíň věcem, co si reálně myslim, že potřebujou. Typicky se tím vyfiltruje ten virus, kterej říká, že je baterka a chce přístup ke všemu. A trackuje tě. Jakoby zkouším ty aplikace, zkouším je zapnout s žádnejma oprávněníma, když vyhoděj chybu, tak jedu dál, ale oni většinou nepotřebujou všechno.*“

Všichni tito studenti používají více hesel se stejným vzorcem – rozlišením důležitosti stránky a informací jí poskytovaných a případně zvolení adekvátně silného hesla. Jako třeba Helena: *„Jako mívám jedno heslo na takový jako nedůležitý věci typu registrace na nějakých hrách, e-shopech, a takový věci. Ale pro Facebook, mail, sis, tam mám všude jiný heslo*.“ Nebo René*: „Pro mě jsou jakoby služby různé úrovně, co maj různou hodnotu. Takže třeba služba třetí úrovně je třeba úplná blbost, kde člověka nutí, aby se registroval na to, aby si mohl přečíst článek, tak tam použiju klidně jako heslo svoje jméno, protože mi to je jedno a přihlašovací e-mail budu mít, případně nějakej nesmyslnej nick. Kterej často zapomenu. Případně používám různé variace.“* Michal: *„Mám spoustu hesel. Mám je zapamatovaný pohybama rukou na klávesnici.* (…) *Silný hesla, ne jméno mý kočky, pokud se kočka nejmenuje xy452szblablabla...* (A tak si představuješ silný heslo?) *„No, ne. Protože pokud se ta kočka fakt tak jmenuje, tak je to blbý, že jo. (smích) Heslo, který nejde najít v žádným slovníku hesel. Tím jsem vyloučil slovníky českýho i jinýho jazyka i všech použitejch hesel.“*

U této skupiny dochází k pocitu smíření s tím, jakým stylem se s uživatelskými daty zachází, co se týče jejich sběru i užití, a důvěry v to, že to není primárně za škodlivým účelem. René si stabilně udržuje jistý nadhled: „*Já jsem se s internetem, jak funguje, smířil vcelku. Dokud mě někdo nepoškodí nějakým způsobem, to znamená já nevim, na tu moji pověst nebo mě neokrade nebo něco takovýho..., tak mi to nevadí*.“ A lakonicky dodává: *„Nebo pokud na základě toho, co jsem dělal, někdo nevyvine způsob, jak ovládat lidstvo, to by mě asi štvalo.*“ Zároveň sbírání jeho dat nevidí jako potenciálně nebezpečné: „*Já bych neřekl, že je to nebezpečný, je to jenom o tom, jestli mi vadí, že se používají uživatelská data o mém procházení nebo ne*.“ Vidí i jeho světlé stránky: „*Já to vim, že ty uživatelský data maj reálný dopad na to, když se potom vyvíjí nějaká aplikace. Jo, sem tam se stane, že se někde změní interface a člověk si říká, jo tohle je dobrý, tohle je blbý, ale přinejmenším podíl může bejt z tohohle*.“

Tito studenti si uvědomují rizika, neodmítají je, avšak snaží se jim aktivně vyhnout a na základě vědomí, že se nechovají nebezpečně, berou tuto problematiku v klidu. Mirek, ač aktivně tvořící a přispívající do Google komunity, si myslí, že pro něj jsou rizika minimální: „*Asi minimální. Jako do účtu se mi asi někdo nabourat nějak může, ale to se může stát komukoliv. Nemyslím si, že bych to riziko nějak zvětšoval*." Ve společnosti ukládající data má důvěru: „*Oni to nezneužijou, otázka je, kdyby to uniklo, co se s tím stane.*" Michal, který uveřejňuje příspěvky na Facebooku a velmi aktivně pracuje s cloudovými službami, má rovněž pocit, že jeho data jsou v bezpečí: *„Myslím si, že to v bezpečí je, ty moje maily asi ještě tolikrát jako hacknutý nebyly, jakoby nikdy jsem neměl žádnou službu hacknutou, na notebooku jsem nikdy žádnej vir neměl, takže v pohodě, no."* I v souvislosti s reklamou a informacemi vedoucí k nim, není jejich postoj striktně negativní, ačkoliv se jejímu zobrazování vyhýbají skrze použití doplňku do prohlížeče Adblock. Josef ví o používání jeho dat: *„Věřím tomu, že je nějak používají... Ale ne konkrétně proti mě..., spíš jako součást dat do data miningu a na cílenou reklamu."* Ale opět je jeho názor na využití dat spíše kladný: *„Myslím, že je to docela dobré... Celkově. Cílená reklama není tak špatná a podporuje to datamining... Ten... Který dává zajímavé výsledky. Studie o tom, jak se lidí chovají, lepší nabízení služeb a tak."*

Strategie těchto respondentů ohledně jejich soukromí je pragmatická dle Dr. Westina a tito respondenti by se dali popsat jako obezřetní, přičemž nejen zvažují výhodnost poměru poskytnutí jejich informací, ale i vědí možná rizika. V oblasti publikování obsahu jsou to sebevědomí kreativci (Pew, 2007), téměř se nebojí o bezpečí svých dat, pokud chtějí, tak aktivně sdílejí, avšak s určitou limitací osobních údajů. (viz kapitola 2.5.1)

Strategie založená na pocitech

Respondenti s nižšími znalostmi své strategie zakládají na své přirozenosti, na pocitech, které ze své aktivity mají. Leckdy postrádají jakoukoliv pevnou strategii na ochranu jejich údajů, sází na to, že nikoho jejich data nezajímají a nemusí se tedy o toto starat, na druhou stranu často z této jejich chybějící strategie vyvěrají pocity nejistoty, silné nedůvěry a provinilosti.

Primární strategie je stejně jako u skupiny s vyšším vědomím založená na nesdílení citlivých údajů, nejlépe však žádných údajů, kdy respondenti připouštějí, že cokoliv pro ně může být potenciálně nebezpečné. Štěpánka vidí největší problém v hromadném ukládání dat velkými společnostmi jako je Google a Facebook: „*Asi se vyvarovat... Hm... těm mainstream stránkám jako je Facebook a vůbec těm stránkám, kde o sobě člověk sdílí strašně moc svých osobních dat. I proto si ho chci zrušit. Prostě se vyvarovat uveřejňováním svých dat. Člověk*

postuje svoji polohu, co kde kdy, v kolik hodin. To mi přijde jako nejvíc nebezpečný.“ Sára si představuje zabezpečení rovněž v nulovém obsahu: „*Zabezpečit? Asi nic nedělat skoro na internetu.“* A jiné možnosti si neuvědomuje*: “Já nevím, jestli třeba já osobně to můžu nějak zabezpečit, jestli jsou na to třeba nějaký programy, který to můžou zabezpečit. Vlastně nevím, jak to zabezpečit. Asi co nejmíň osobních informací dávat na internet*.“ Podle Tomáše je nejbezpečnější vůbec žádnou digitální stopu nevytvářet: „*No, žádnou nevytvářet. Že bych nechodil na internet.*“

Dále se ale jejich reálné zabezpečující chování liší. Pro celou skupinu je charakteristické vědomí toho, že by měli na svých účtech mít odlišná silná hesla, avšak nenásledování tohoto pravidla. Tereza si je poměrně jistá v tom, jak by mělo vypadat bezpečné heslo: „*Tak aby to heslo mělo v sobě nějaké číslice, nebo nějaké jiné znaky*.“ Nicméně sama od sebe dodává, že ona to takhle nemá: *„A pak mít asi na každý účet jiné heslo, ale takhle já… uhm... úplně teda nefunguju... Já mám jedno heslo na všechno tak ňák.*“ Tomáš oznamuje: „*Mám jedno heslo, pro jistotu si ho ještě zapíšu*.“

Podobně to má i Sára: „*Takže ty, co tam mám, tak většinou používám stejný heslo. (...) Což je hrozný. A jméno taky většinou používám pořád to samý, nevytvářím si nový, no*.“ Vyslovení tohoto faktu je běžně váhavé, nejisté, emočně zabarvené jistou provinilostí. Štěpánka ví, že by neměla mít na všechny účty jedno heslo, což v ní vyvolává právě pocity viny: „*Já jsem na tohle strašná, já mám všude stejný heslo. Vím, že je to špatný, ale já mám s tímhle problém, že si to pak nepamatuju*.“

K tzv. strategii jednoho hesla respondenti přistupují především kvůli tomu, že se jim zdá nemožné si více přihlašovacích údajů zapamatovat, ale také kvůli již zmíněnému pocitu vlastní nedůležitosti, jako třeba právě Štěpánka, která se uklidňuje, že ač vidí užívání jednoho hesla jako slabé bezpečnostní opatření, tak to nevadí, protože stejně nechrání nic pro ni důležitého: „*Jako ty ty hesla jsou hodně blbý. Ale nikdo nemá důvod mi něco ukrást. Nemyslím si, že bych tam mělo něco až tak životně důležitýho, že kdyby se něco podělalo, tak mě to prostě položí.*“ Sára říká: „*Já jsem pro ně malá ryba*.“ a označením „ně“ shrnuje všechny velké společnosti i potenciální útočníky.

Tito respondenti na základě své nízké důvěry v bezpečí jejich uchylují i k zabezpečujícím aktivitám. Honza pravidelně promazává lokálně uložená data na jeho počítači: „*Co dělám já, že každé dva tři týdny vymažu historii a ty soubory cookies.“* Sára se snaží instalovat aplikace pouze od ověřených dodavatelů: „*Já se většinou snažím stahovat takový, co už maj nějaký lidi stažený, nestahuju si takový neznámý, co maj dvě hvězdičky nebo*

tak. Ale vzhledem k tomu, že jsem slyšela, že si kupujou to hodnocení na tom googlu, no, tak nevím...“ Obvykle pak uživatel přizná, že si není jist důsledkem své akce jako třeba Aneta, která říká: „*Pak mažu historii prohlížeče.“* Poté však dodává, že vlastně neví, proč to dělá: *„To nevím, jestli nějak pomáhá, když si to pravidelně promazáváš, asi moc ne, co? Tak to asi dělám, ale asi je to stejně jedno*.“ I tito studenti většinou zjišťují informace, které jsou o nich dostupné na internetu v podobě ego searchingu, jejich motivace je ale spíše zvědavost než bezpečnost, jak tvrdí Tereza: „*Jako zkoušela jsem to. (smích) Ale to jenom, že jsem se nudila*.“

Již v části zabývající se vědomím uživatelů o zanechávání digitální stopy byl identifikován jev vědomí vlastní nevědomosti. Součástí strategie těchto studentů často není své vědomí rozšiřovat. Tereza při reflexi jejího povědomí o ukládání a zacházení s informace na internetu: „*No, když teď tak nad tím uvažuju... (Smích.) Tak asi to taková sláva nebude, ale nevim... Asi jsem nad tím zatím moc neuvažovala a říkala jsem si, že je to snad v pořádku, ale když teď nad tím tak přemýšlím, tak nevím...*“ V závěrečné části rozhovoru dodává, že jí její znalost nepřijde dostatečná, avšak rozvíjet se nijak neplánuje. Stejně tak Tomáš na otázku „Přijde ti znalost této tématiky dostatečná?“ odpovídá: „*Ne*“, přičemž stručné odpovědi „*Ne*“ se dočká i otázka „Budeš se v ní dál nějak rozvíjet?“ Aneta odpovídá „*Asi bych chtěla. Nevím no*.“ Důvody, proč se tito respondenti aktivně nezajímají a ani zajímat neplánují, shrnuje Štěpánka: *„No... Jelikož si furt myslím, že se na tom internetu chovám tak, že nejsem sama sobě nebezpečná, tak se o to ani moc nezajímám. Kdybych tam něco měla, tak se asi zajímám víc.*“ Vzhledem k tomu, že tito respondenti nepovažují informace, které sdílejí, za zneužitelné, resp. nebezpečné, nepřipadá jim ani důležité se o toto zajímat a dále se vzdělávat.

Většinu uživatelů z této skupiny můžeme zařadit dle typologie PEW (PEW, 2007) do třídy „Ustaraní na vedlejší koleji“, kdy se tito studenti tedy do určité míry strachují o své soukromí na internetu, avšak významně jej nelimitují a nepociťují potřebu se významněji starat. Výjimkou v této kategorii je Honza, který sám sebe popisuje: „*Dá se to tak říct, že jsem tak trošku paranoidní. (smích) Vím, že nejsem až takový... Že nemám až takové vědomosti o tom, jak toto funguje, ale prostě to, co můžu, tak se snažím... snažím... nějak udržet pod kontrolou.*“, jež by se spíše hodil do kategorie Znepokojení a opatrní.

4.6. Shrnutí výzkumu

Uživatelské chování studentů na webu bylo analyzováno skrze polostrukturované rozhovory. Rozhovorům předcházela rešerše literatury shrnující tématiku digitálních stop a uživatelského chování, na jejichž základě byla sestavena kostra rozhovoru. Během nich

docházelo simultánně k přepisu a předběžné analýze, na základě které došlo nakonec k patnácti sezením s různými studenty.

Během rozhovorů byly postupně utvářeny konstrukce zjištěných informací. Ač byla zaznamenána rozdílná úroveň znalostí o ukládání digitální stopy, žádný ze studentů nebyl úplně bez nich. Z rozdílných znalostí vyplývala rozdílná důvěra v bezpečnost internetu a z rozdílné důvěry vycházely odlišné strategie uživatelského chování. Právě strategie uživatelského chování či její neexistence tvoří primární zjištění této práce.

4.6.1. Odpovědi na výzkumné otázky

Klíčová výzkumná otázka, od které se ubíral celý směr výzkumu, zněla: **V jakém rozsahu si studenti uvědomují, že po sobě zanechávají na internetu digitální stopu?**

Pro odpověď na tuto otázku se musíme oprostit od pojmu „digitální stopa“, protože ani samotní studenti tento pojem nepoužívají a neznají. Úplně všichni zpovídaní studenti si byli vědomi zanechávání aktivní digitální stop a toho, že tato aktivně vložená stopa není v jejich vlastnictví, jakmile se jednou uloží.

Ohledně ukládání pasivní stopy je škála znalostí rozmanitější. Naprostá většina studentů si uvědomuje její zanechávání, resp. zaznamenávání, alespoň ve spojitosti s cílenou reklamou. Avšak tito studenti se ve svých znalostech liší, přičemž polovina má o ukládání pasivní digitální stopy hrubé představy založené na útržkovitých informacích získaných od svého okolí. Pouze menšina studentů vidí detailněji do mechanismů ukládání digitálních stop a uvědomuje si jejich rozsah v celé jejich šíři.

Tabulka 6 Rozvrstvení znalostí u sledovaného vzorku

	Aktivní digitální stopa	Pasivní digitální stopa	
Představa		Hrubá	Detailní
Uvědomuje si:	15	8	4

Vědí, kdo všechno má přístup k jejich digitálním stopám? Studenti s vyššími znalostmi si uvědomují i přístup třetích stran k jejich digitálním stopám. Ale většina studentů si není vůbec jistá, kdo jejich data kam ukládá.

Druhou výzkumnou otázkou byla: **Jaký dopad mají znalosti o digitální stopě na respondentovo uživatelské chování na internetu?**

Studenti s vyššími znalostmi o ukládání digitální stopy byly v jejich jednání mnohem jistější, vědomí toho, jak kam a kým se jejich digitální stopa ukládá, v nich vyvolávalo jistotu a větší důvěru v to, že jejich informace jsou na internetu v bezpečí, neomezovali tedy velmi svoji aktivitu a volně publikovali i veřejný obsah. Nízké znalosti naopak vyvolávaly nejistotu a nedůvěru, tito uživatelé se snaží nevypouštět žádné informace na internet.

Jakým způsobem budují svoji digitální stopu? Studenti digitální stopu nebudují cíleně, nesnaží se svoji digitální stopu cíleně rozšiřovat a tvarovat. Svým aktivitám na internetu nechávají volný průběh, většinou však necítí potřebu se veřejně seberealizovat či prezentovat na internetu.

Jak (pokud vůbec) se snaží své digitální stopy chránit? V oblasti ochrany digitálních stop studenti rozlišují dvě strategie, obě jsou založeny na ochraně citlivých údajů – primárně jejich neuveřejňování. Studenti s nižšími znalostmi se omezují na minimální aktivitu, mají pocit, že je to ochrana na dostatečné úrovni vyhovující jejich potřebám. Strategie studentů s vyššími znalostmi dále upřednostňuje nad neuvolňováním citlivých údajů ochranu těch informací, které studenti již na internet umístili. Tato strategie je založena na důsledném dodržování pravidel bezpečného chování na internetu. Tito studenti vědí, jak své informace chránit a také tak činí – mají kvalitně zabezpečené účty, kontrolují soukromí a zabezpečení aplikací a stránek.

4.6.2. Další zjištění

Rozdělení studentů podle míry znalostí z předcházejících kapitol se ukázalo jako velmi funkční. Obě skupiny – ta s minimálními a průměrnými znalostmi a ta s nadprůměrnými a vysokými znalostmi – vykazovaly stejné vzorce chování. Více uvědomělí pracovali podle jasně stanovené strategie, obsahující dodržování bezpečného chování na internetu a přijímání pravidel, podle kterých internet funguje. Méně uvědomělí neměli vytvořenou téměř žádnou strategii a jejich chování bylo více náhodné, založené na tom, co někde vyslechli či náhodou vyčetli.

Jedním z důležitých vlivů na studenty, který byl identifikován během výzkumného šetření, byl pocit vlastní nedůležitosti. Tento pocit měl však mnohem větší vliv na chování méně uvědomělých uživatelů, kdy na tomto pocitu zakládali „strategii jednoho hesla“, málokterému studentu z této skupiny také přišla tématika bezpečnosti na internetu důležitá, ačkoliv přiznávali, že si jsou vědomi, že jí příliš nerozumí a nemyslí si, že by jejich informace byly na internetu v bezpečí.

Pokud nahlédneme do proběhnutých rozhovorů za účelem zjištění příčin rozporuplnosti a diametrálně odlišných strategií, můžeme zjistit, že ani jeden ze studentů neprošel vzdělávací akcí v rámci středoškolského či vysokoškolského studia. Znalosti studentů o ukládání digitální stopy a její ochrany tedy závisí především na studentově zájmu. Což bylo dokázáno i v samotných rozhovorech, kdy v závěrečné části věnované právě zájmu studentů o zkoumanou tématiku, projevovali studenti s vyššími znalostmi i vyšší zájem.

4.6.3. Omezení zjištěných informací

Zkoumané téma bylo pro některé studenty velmi složité, otázky byly koncipovány tak, aby se co nejvíce vyhnuly jakékoliv terminologii, které by student nemusel rozumět, avšak i tak byl student konfrontován s oblastmi, nad kterými nikdy nepřemýšlel. K této překážce došlo především s respondenty, kteří měli minimální znalosti o ukládání digitální stopy.

Nicméně vzhledem k tomu, že primárním cílem práce bylo zjištění stavu znalostí a reálného chování, byl rozhovory vzaty v potaz v takové podobě, v jaké byly, neboť nejlépe reprezentovaly stav respondenta před provedením rozhovoru. Někteří respondenti totiž po dokončeném rozhovoru projevili mírný zájem o tuto tématiku, který by bez jeho provedení pravděpodobně běžně neprojevili.

4.6.4. Využitelnost a možnosti pro dalšího výzkum

Z hlediska převedení zjištění do praktických poznatků lze poukázat na nesoudržnost vysokoškolských studentů, kdy vyšší znalosti mají pouze ti s vyšším zájmem, v kombinaci s tím, že žádný z dotazovaných studentů neabsolvoval systematickou výuku v oblasti digitálních stop. Z tohoto hlediska by výsledek tohoto výzkumu nabádal k větší integraci této tématiky do středoškolských osnov, popř. je na povážení i jeho zavedení v rámci přednášek vysokoškolských či programu vysokoškolských knihoven.

Před takovýmto krokem by však bylo nutno zvážit dva další aspekty. Aktuální stav výuky na středních školách, který nebyl předmětem této práce (a tudíž jej nelze předpokládat bez bližšího prozkoumání). A nástup příslušníků internetové generace na vysoké školy. Tedy osob narozených po roce 1995, které vyrůstaly s vlivem internetu v podstatě již od kolébky, přičemž tento výzkum byl veden se skupinou studentů narozených převážně před tímto rokem a vzorce jejich chování se mohou lišit.

Pro doplnění závěrů z výzkumu doporučujeme provedení opakovaných rozhovorů s respondenty s nižšími znalostmi. Jednalo by se o sérii rozhovorů identifikující znalosti a

uživatelské chování, přičemž po rozhovoru by následovala volná diskuze s respondentem za účelem mu objasnit zákonitosti digitálních stop a zvýšit jeho znalosti. Po určitém intervalu by se s daným respondentem rozhovor zopakoval a bylo by sledováno, zda mělo zvýšení jeho znalostí nějaký vliv na jeho chování.

Závěr

Za účelem analýzy uživatelského chování byla nejdříve v teoretické části podrobně prozkoumána problematika digitální stopy s důrazem na procesy s nimi spojenými. Digitální stopy se vyskytují v aktivní formě, kdy uživatel proaktivně umisťuje na internet nějaký obsah, a pasivní, kdy je sledováno především uživatelovo chování – na které byl brán zřetel. Na část o digitálních stopách bylo navázáno studií uživatelského chování skrze rešerši odborných zdrojů a výčtem možností, které moderní digitální prostředí uživatelům nabízí.

Při monitoringu odborné literatury proběhla i rešerše výzkumů a kvalifikačních prací, které se zabývají podobnou tématikou – tedy uživatelským chováním v souvislosti s digitálními stopami, tento monitoring přinesl obrázek současného stavu a zájmu.

K analýze bylo přikročeno skrze kvalitativní metodologii, která byla zvolena kvůli bližšímu kontaktu s respondentem. S ním byl veden polostrukturovaný rozhovor, který měl tři části – první se zabýval aktivitou respondenta na internetu, druhý identifikací jeho znalostí o ukládání jeho digitální stopy a finální třetí vztahem mezi respondentovou aktivitou a jeho znalostmi. Za účelem shromáždění dostatečného množství dat bylo nakonec uskutečněno patnáct rozhovorů.

Cílem práce bylo identifikovat, jak a do jaké míry ovlivňují aktivní znalosti o ukládání digitální stopy uživatele jeho chování. Za tímto účelem byli položeny dvě výzkumné otázky: V jakém rozsahu si studenti uvědomují, že po sobě zanechávají na internetu digitální stopu? a Jaký dopad mají jejich znalosti na jejich uživatelské chování na internetu?

Přičemž bylo zjištěno, že si studenti dobře uvědomují ukládání jejich aktivní digitální stopy, avšak, co se týče pasivní digitální stopy, nebyli studenti jednotní. Byly identifikovány dvě skupiny studentů – jedna s vysokými znalostmi a druhá s nižšími, většinou omezenými na propojení digitální stopy s cílenou reklamou.

Na základě rozdělení uživatelů dle míry znalostí byla rozpoznána i závislost mezi reálným chování a znalostmi. Přičemž studenti s vyššími znalostmi se na jednu stranu chovali bezpečněji (dodržovali zásady bezpečného chování na internetu) a na druhou také s větší důvěrou v bezpečí jejich informací, tedy poměrně volně publikovali obsah, a to i veřejně. Skupina s nižšími znalostmi měla ohledně ukládání digitální stopy pocity nedůvěry a nejistoty vyplývající právě z jejich nízkých znalostí. Navzdory tomuto pocitu se běžně nepokoušeli jejich informace na internetu chránit, protože měli pocit, že tyto informace vlastně nikoho nezajímají.

Výsledků této práce lze použít jako východiska pro další práci se znalostmi uživatelů o digitální stopě, především ve výuce na středních a vysokých školách, neboť chování uživatelů s nižšími znalostmi obsahovalo i potenciálně nebezpečné chování spočívající v nedostatečném zabezpečení jejich účtů, bezmyšlenkovým povolováním přístupů programům. Několik uživatelů – výhradně právě s nižšími znalostmi – přiznalo špatnou zkušenost v souvislosti s jejich digitálním životem a je znepokojující to, že ani jejich vlastní zkušenosti je nepřiměli svoje znalosti prohloubit.

Seznam použité literatury

- ACMA. 2013. *Digital footprints and identities: Community attitudinal research*. Melbourne, 2013. Dostupné také z: http://www.acma.gov.au/~/media/Regulatory%20Frameworks%20and%20International%20Engagement/Information/pdf/Digital%20footprints%20and%20identities%20community%20attitudinal%20research%20pdf.
- ASHTON, Kevin. 2010 That 'Internet of Things' thing. *RFID Journal* [online]. 2010 [cit. 2017-06-16]. Dostupné z: http://www.itrco.jp/libraries/RFIDjournal-That%20Internet%20of%20Things%20Thing.pdf.
- BATTELLE, John. 2004 From the Ephemeral to the Eternal. In: *Search blog* [online]. 2004 [cit. 2017-06-16]. Dostupné z: http://battellemedia.com/archives/2004/05/from_the_ephemeral_to_the_eternal.php.
- BERNERS-LEE, Tim, James HENDLER a Ora LASSILA. The Semantic Web. Scientific American [online]. Primosig, 2001, 284(5), 35-43 [cit. 2017-06-16]. Dostupné z: https://pdfs.semanticscholar.org/566c/1c6bd366b4c9e07fc37eb372771690d5ba31.pdf.
- BODOVSKAYA, E., A. DOMBROVSKAYA a R. GIBAULIN et al. 2016 Internet-Behavior Typology and Characteristic Features: Cross-National Comparative Analysis. *Global Media Journal* [online]. 2016, **14**(27) [cit. 2017-06-22]. ISSN 1550-7521. Dostupné z: http://www.globalmediajournal.com/open-access/internetbehavior-typology-and-characteristic-features-crossnational-comparative-analysis.php?aid=83237.
- CAMACHO, Mar, Janaina MINELLI a Gabriela GROSSECK. 2012. Self and Identity: Raising Undergraduate Students' Awareness on Their Digital Footprints. *Procedia - Social and Behavioral Sciences* [online]. 2012, **46**, 3176-3181 [cit. 2017-06-16]. DOI: 10.1016/j.sbspro.2012.06.032. ISSN 1877-0428. Dostupné z: http://linkinghub.elsevier.com/retrieve/pii/S1877042812017685.
- Cambridge Semantics. Introduction to the Semantic Web. In: *Cambridge Semantics* [online]. Cambridge, 2017 [cit. 2017-06-16]. Dostupné z: http://www.cambridgesemantics.com/semantic-university/introduction-semantic-web.
- ČESKÝ STATISTICKÝ ÚŘAD. 2015. *Čas strávený na internetu jednotlivci v České republice pro soukromé účely; 2. čtvrtletí 2015*. Praha, 2015. Dostupné také z: https://www.czso.cz/documents/10180/20568879/062004-1521.pdf/e1f5945f-4b1c-4915-b3a4-bbfeec155ab2?version=1.0.
- ČESKÝ STATISTICKÝ ÚŘAD. 2016. *Využívání informačních a komunikačních technologií v domácnostech a mezi jednotlivci*. Praha, 2016. Dostupné také z: https://www.czso.cz/documents/10180/50104893/062004-16c.pdf/443e2843-2566-4848-bf27-db72a610fe43?version=1.2.
- Digital footprint. 2016. In: *Salem Press Encyclopedia,* [online]. Salem Press, 2016 [cit. 2017-06-16]. Dostupné z: http://www.salempress.com/%20digital%20footprint.
- DISMAN, Miroslav. Jak se vyrábí sociologická znalost: příručka pro uživatele. Miroslav Disman. 3. vyd. Praha: Karolinum, 2002. 374 s.
- DONOVAN, Gregory Thomas. *MyDigitalFootprint.ORG: Young People and the Proprietary Ecology of Everyday Data*. New York, 2013. Dostupné také z: http://academicworks.cuny.edu/gc_etds_legacy/1. Disertační práce. City University of New York. Vedoucí práce Cindi Katz.

- EMC Digital Universe. Data Growth, Business Opportunities, and the IT Imperatives. In: *EMC Digital Universe* [online]. 2014 [cit. 2017-06-22]. Dostupné z: https://www.emc.com/leadership/digital-universe/2014iview/executive-summary.htm.
- *Encyklopedický slovník*. Praha: Odeon, 1993. Klub čtenářů (Odeon). ISBN 80-207-0438-8.
- ERDELEZ, Sandra. 1999. Information Encountering: It's More Than Just Bumping into Information. *Bulletin of the American Society for Information Science and Technology* [online]. 1999, **25**(3), 26-29 [cit. 2017-06-22]. DOI: 10.1002/bult.118. ISSN 00954403. Dostupné z: http://doi.wiley.com/10.1002/bult.118.
- Facebook. 2017. Přístup k osobním údajům na Facebooku. *Facebook* [online]. 2017 [cit. 2017-06-22]. Dostupné z: https://www.facebook.com/help/405183566203254.
- FISH, Tony. 2009. *My digital footprint: a two sided digital business model where your privacy will be someone else's business*. London: Futuretext, 2009. ISBN 978-095-5606-984.
- FISHER, Karen E., Sanda ERDELEZ a Lynne MCKECHNIE, ed. *Theories of information behavior*. Medford: Information Today, c2005. ASIST monograph series. ISBN 15-738-7230-X.
- GARDELKA, Tomáš. 2016. Kolektivní inteligence. In: *Transpersonální forum* [online]. 2016 [cit. 2017-06-22]. Dostupné z: http://www.tacz.org/integralni-kultura/kolektivni-inteligence.
- GARFINKEL, Simon a David COX. 2009. *Finding and Archiving the Internet Footprint*. Monterey, 2009. Dostupné také z: https://simson.net/clips/academic/2009.BL.InternetFootprint.pdf.
- GEARY, Joanna. 2012. Tracking the trackers: What are cookies? An introduction to web tracking. In: *The Guardian* [online]. 2012 [cit. 2017-06-22]. Dostupné z: https://www.theguardian.com/technology/2012/apr/23/cookies-and-web-tracking-intro.
- GOLDER, Scott A. a Michael W. MACY. 2013. Social Media as a Research Environment. *Cyberpsychology, Behavior, and Social Networking* [online]. 2013, **16**(9), 627-628 [cit. 2017-03-02]. DOI: 10.1089/cyber.2013.1525. ISSN 2152-2715. Dostupné z: http://online.liebertpub.com/doi/abs/10.1089/cyber.2013.1525.
- GOLDER, Scott A. a Michael W. MACY. 2014. Digital Footprints: Opportunities and Challenges for Online Social Research. *Annual Review of Sociology* [online]. 2014, **40**(1), 129-152 [cit. 2017-03-02]. DOI: 10.1146/annurev-soc-071913-043145. ISSN 0360-0572. Dostupné z: http://www.annualreviews.org/doi/10.1146/annurev-soc-071913-043145.
- GOODIER, Holly. BBC Online Briefing Spring 2012: The Participation Choice. In: *BBC* [online]. 2012 [cit. 2017-06-25]. Dostupné z: http://www.bbc.co.uk/blogs/bbcinternet/2012/05/bbc_online_briefing_spring_201_1.html.
- GOOGLE. Cit. 2017a. Zobrazení dat a aktivity na účtu na Hlavním panelu Google. *Nápověda účet Google* [online]. [cit. 2017-06-25]. Dostupné z: https://support.google.com/accounts/answer/162744?hl=cs&ref_topic=7188671.
- GOOGLE. Cit. 2017b. Jak fungují reklamy: Vaše osobní údaje nikomu neprodáváme. *Reklamy Google* [online]. [cit. 2017-06-25]. Dostupné z: https://privacy.google.com/intl/cs/how-ads-

work.html?utm_source=google&utm_medium=ad-settings&utm_campaign=inbound-site-link.

- GOOGLE. Cit. 2017c. Chraňte svoje bezpečí a soukromí. *Google* [online]. [cit. 2017-06-25]. Dostupné z: https://www.google.cz/safetycenter/everyone/start.
- GOOGLE. Cit. 2017d. Ochrana soukromí a smluvní podmínky. Google [online].]. [cit. 2017-06-25]. Dostupné z: https://www.google.com/intl/cs/policies.
- GORDIC. 2017. Průzkum o chování českých uživatelů internetu. In: GORDIC SPOL. S R. O. *IT point* [online]. 2017 [cit. 2017-06-25]. Dostupné z: http://www.itpoint.cz/gordic/clanky/?i=chovani-uzivatelu-internetu-pruzkum-11514.
- GONTOVNIKAS, Martin. 2016. Why Federated Identity Management Matters. In: *Auth0* [online]. 2016 [cit. 2017-06-25]. Dostupné z: https://auth0.com/blog/why-identity-federation-matters.
- HEKTOR, Anders. 2003. Information activities on the Internet in everyday life. *The New Review of Information Behaviour Research* [online]. 2003, **4**(1), 127-138 [cit. 2017-06-25]. DOI: 10.1080/14716310310001631480. ISSN 1471-6313. Dostupné z: http://www.tandfonline.com/doi/abs/10.1080/14716310310001631480.
- HERMAN, Ivan. 2009. *Introduction to the Semantic Web*. San Jose, 2009. Dostupné také z: https://www.w3.org/2009/Talks/0615-SanJose-tutorial-IH/Slides.pdf.
- HENDL, Jan. 2005. *Kvalitativní výzkum: základní metody a aplikace*. Praha: Portál, 2005, s. 168 - 172. ISBN 80-7367-040-2.
- CHUN-YAO, H, YUNG-CHENG, S, I.-PING, C, a CHEN-SHUN, L. 2007. Characterizing Web users online information behavior. *Journal Of The American Society For Information Science & Technology.* 2007, **58**(13), s. 1988-1997.
- JONÁK, Zdeněk. 2003. Informační chování. In: KTD: Česká terminologická databáze knihovnictví a informační vědy (TDKIV) [online]. Praha : Národní knihovna ČR, 2003- [cit. 2017-03-23]. Dostupné z: http://aleph.nkp.cz/F/?func=direct&doc_number=000000463&local_base=KT.
- JONÁK, Zdeněk. 2003. Znalost. In: *KTD: Česká terminologická databáze knihovnictví a informační vědy (TDKIV)* [online]. Praha : Národní knihovna ČR, 2003- [cit. 2017-06-29]. Dostupné z: http://aleph.nkp.cz/F/?func=direct&doc_number=000000498&local_base=KTD.
- DE KERCKHOVE, D a DE ALMEIDA, C. 2013. What is a digital persona*? Technoetic Arts: A Journal Of Speculative Research*. 2013 **11**(3), 277-287. [cit. 2017-04-05] Dostupné z: Academic Search Complete, EBSCOhost.
- KIRK, Jeremy. 'Canvas fingerprinting' online tracking is sneaky but easy to halt. In: *PC World* [online]. Austrálie, 2014 [cit. 2017-07-10]. Dostupné z: http://www.pcworld.com/article/2458280/canvas-fingerprinting-tracking-is-sneaky-but-easy-to-halt.html.
- KRHOVJÁK, J. a MATYÁŠ, Václav. 2007. Autentizace a identifikace uživatelů. *Zpravodaj ÚVT MU*. 2007 **18**(1), 1-5. ISSN 1212-0901 Dostupné z: http://webserver.ics.muni.cz/bulletin/articles/560.html.
- KRISHNAN, Hari. Defending yourself from Google hackers. In: *Infosec Institute* [online]. Madison, 2012 [cit. 2017-07-11]. Dostupné z: http://resources.infosecinstitute.com/defending-from-google-hackers.
- KROPÁČOVÁ, Andrea. 2014. CESNET, Z. S. P. O. *Základy bezpečnosti v IT: Informované užívání Internetu jako nejlepší prevence*. Praha, 2014.

- KŘÍŽ, Lukáš. 2014. Na webu beze stop. *Česká pozice: Informace pro svobodné lidi* [online]. [cit. 2016-05-09]. Dostupné z: http://ceskapozice.lidovky.cz/na-webu-beze-stop-0eg-/tema.aspx?c=A141218_143545_pozice-tema_kasa.
- KUMARAGURU, Ponnurangam. 2005. *Privacy indexes: a survey of Westin' s studies*. Mellon, 2005. Doi 10.1.1.464.9348. Dostupné komerčně z: http://citeseerx.ist.psu.edu.
- Deyi Li, Liwei Huang. 2012. Interaction and Collective Intelligence on the Internet. In: *Agrawal M., Cooper S.B., Li A. (eds) Theory and Applications of Models of Computation. TAMC 2012. Lecture Notes in Computer Science, vol 7287*. Springer, Berlin, Heidelberg. Dostupné komerčně z: https://link.springer.com.
- JŠNSSON, Tove. 2014. Three types of user behavior that you should know about if you conduct online research. In: *E -marketing Blog* [online]. Utrecht, 2014 [cit. 2017-07-11]. Dostupné z: http://emarketingblog.nl/2014/12/three-types-of-user-behavior-that-you-should-know-about-if-you-conduct-online-research.
- LANCIERI, Luigi a Nicolas DURAND. 2006 Internet User Behavior: Compared Study of the Access Traces and Application to the Discovery of Communities. *IEEE transactions on systems, man, and cybernetics. Part A: Systems and humans* [online]. 2006, **36**(1) [cit. 2017-07-11]. ISSN 1083-4427. Dostupné z: http://nicolas.durand.perso.luminy.univmed.fr/docs/ld_tsmc2006.pdf.
- LAUBE, David. 2015. Nová média shromažďující informace o svém publiku a vztah uživatelů k bezpečnosti dat: kvalitativní studie. Ústí nad Labem, 2015. 80 s. Diplomová práce (Mgr.) Univerzita Karlova, Fakulta sociálních věd, Institut komunikačních studií a žurnalistiky. Katedra mediálních studií. Vedoucí diplomové práce Mgr. Jaroslav Švelch, PhD.
- LANDOVÁ, Hana. 2002. Kdo, kde a jak řeší problém informační gramotnosti?. *Ikaros* [online]. 2002, **6**(9) [cit. 2017-06-13]. urn:nbn:cz:ik-11000. ISSN 1212-5075. Dostupné z: http://ikaros.cz/node/11000.
- LEHMAN, Tomáš. 2014. Analýza chování uživatelů sociální sítě Facebook. Praha, 2014. Diplomová práce (Ing.). Vysoká škola ekonomická v Praze. Vedoucí práce Tomáš Sigmund.
- LÉVY, Pierre. *Collective intelligence: mankind's emerging world in cyberspace*. Cambridge, Mass.: Perseus Books, c1997. ISBN 07-382-0261-4.
- LIEM, Cassandra a Georgios PETROPOULOS. The economic value of personal data for online platforms, firms and consumers. In: *Bruegel* [online]. Brussel, 2016 [cit. 2017-07-11]. Dostupné z: http://bruegel.org/2016/01/the-economic-value-of-personal-data-for-online-platforms-firms-and-consumers.
- LINDEROVÁ, Ivica, Petr SCHOLZ a Michal MUNDUCH. Úvod do metodiky výzkumu. Jihlava: Vysoká škola polytechnická Jihlava, 2016. ISBN 978-80-88064-23-7.
- LOPEZ RESEARCH. *An Introduction to the Internet of Things (IoT)*. San Francisco, 2013. Dostupné také z: http://www.cisco.com/c/dam/en_us/solutions/trends/iot/introduction_to_IoT_novembe r.pdf.
- MADDEN, Mary, Susannah FOX, Aatron SMITH a Jessica VITAK. 2007. *Digital Footprints: Online identity management and search in the age of transparency*. Washington, 2007. Dostupné také z: http://www.pewinternet.org/files/old-media/Files/Reports/2007/PIP_Digital_Footprints.pdf.
- MADDOX, Maeve. 2014. Person vs. Persona. In: *Daily Writing Tips* [online]. 2014 [cit. 2017-07-11]. Dostupné z: https://www.dailywritingtips.com/person-vs-persona.

- MALONE, Thomas W. 2012. Collective Intelligence. In: *Edge* [online]. 2012 [cit. 2017-07-11]. Dostupné z: https://www.edge.org/conversation/thomas_w__malone-collective-intelligence.
- MARKELZ, Michelle. 2016. Digital Tracking Technologies: A Primer. In: *American Marketing Association* [online]. Chicago, 2016 [cit. 2017-07-11]. Dostupné z: https://www.ama.org/publications/MarketingNews/Pages/digital-tracking-technology-basics.aspx.
- MILES, M. a B., HUBERMANN. 1994. *Qualitative data analysis. A sourcebook of new methods*. London: Sage, 1994.
- MEYEN, Michael, Senta PFAFF-RÜDIGER, Kathrin DUDENHÖFFER a Julia HUSS. 2010. The internet in everyday life: a typology of internet users. *Media, Culture* [online]. 2010, **32**(5), 873-882 [cit. 2017-07-11]. DOI: 10.1177/0163443710374792. ISSN 0163-4437. Dostupné z: http://journals.sagepub.com/doi/10.1177/0163443710374792.
- MEDIAN. 2017. *E-Government, bezpečnost na internetu: Výzkum internetové populace*. Praha, 2017. Dostupné také z: http://www.median.eu/cs/wp-content/uploads/2017/02/Kyberneticke_hrozby_MEDIAN_leden_2017.pdf.
- NATIONS, Daniel. What Is Web 3.0 and Is It Here Yet? In: *Lifewire* [online]. 2017 [cit. 2017-07-11]. Dostupné z: https://www.lifewire.com/what-is-web-3-0-3486623.
- NCACIC - National Cybersecurity and Communications Integration Center. 2014. Digital footprint: assessing risk and impact [online]. [cit. 2015-05-09]. Dostupné z: https://www.urmc.rochester.edu/MediaLibraries/URMCMedia/flrtc/documents/IT-20140218_Digital-Footprint.pdf.
- NPR. 2016. Online Trackers Follow Our Digital Shadow By 'Fingerprinting' Browsers, Devices. In: NPR. *All Tech Considered* [online]. 2016 [cit. 2017-07-11]. Dostupné z: sections/alltechconsidered/2016/09/26/495502526/online-trackers-follow-our-digital-shadow-by-fingerprinting-browsers-devices.
- O'REILLY, Tim. 2009. What Is Web 2.0: Design Patterns and Business Models for the Next Generation of Software. *International Journal of Digital Economics. 2009,* **65**, 17-37. Dostupné z: https://mpra.ub.uni-muenchen.de/4580.
- OSBORNE, Nicola a Louise CONNELLY. 2015. *Managing your digital footprint: possible implications for teaching and learning*. Porto, 2015.
- OSBORNE, Nicola a Louise CONELLY. *Students' Digital Footprints: Curation of Online Presences, Privacy and Peer Support*. Caen, 2016.
- OSBORNE, Nicola a Louise CONNELLY. 2015b. *Student identities in transition: social media experiences, curation, and implications for higher education*. Sheffield, 2015.
- POSTSCAPES. 2017. An Internet of Things. In: POSTSCAPES. *Postscapes* [online]. 2017 [cit. 2017-07-11]. Dostupné z: https://www.postscapes.com/internet-of-things-examples.
- PRENSKY, Marc. Digital Natives, Digital Immigrants. *On the Horizon*. MCB University Press, 2001, **9**(5). Kopie dostupná z: http://www.marcprensky.com/writing/Prensky%20-%20Digital%20Natives,%20Digital%20Immigrants%20-%20Part1.pdf.
- RUDMAN R.J. 2010. Incremental negative impacts in Web 2.0 applications. *The Electronic Library*, 2010 **28**(2), 210-230.). ISSN 0264-0473.
- RUDMAN, R. a BRUWER, R. 2016. Defining Web 3.0: Opportunities and Challenges. *The Electronic Library*, 2016, **34(**1), 132-154.). ISSN 0264-0473. Dostupné komerčně z: Library & Information Science Abstracts (LISA).

- SIPIOR, J, B.WARD a R.MENDOZA. 2011. Online Privacy Concerns Associated with Cookies, Flash Cookies, and Web Beacons', *Journal of Internet Commerce* [online]. 2011. 10(1), 1-16. [cit. 2017-07-11] DOI 10.1080/15332861.2011.558454.
- Mats SJÖBERG a kol. 2016. *Digital Me: Controlling and Making Sense of My Digital Footprint*. Helsinki, 2016. Dostupné také z: https://www.cs.helsinki.fi/u/mvsjober/papers/dime-paper-symbiotic2016.pdf.
- SKLENÁK, Vilém a Ludmila CELBOVÁ. Internet. *In*: KTD: Česká terminologická databáze knihovnictví a informační vědy (TDKIV) [online]. Praha : Národní knihovna ČR, 2003- [cit. 2017-03-23]. Dostupné z: http://aleph.nkp.cz/F/?func=direct&doc_number=000000536&local_base=KT.
- STRICKLAND, Jonathan. How Web 2.0 Works. In: *Tech* [online]. Atlanta, 2007 [cit. 2017-07-11]. Dostupné z: http://computer.howstuffworks.com/web-20.htm.
- SPEICHER, Max. The Arrival of the Web 3.0. In: *Medium* [online]. Michigan, 2016 [cit. 2017-07-11]. Dostupné z: https://medium.com/@maxspeicher/the-arrival-of-the-web-3-0-e826b0913ddd.
- SPRENGER, Polly. Sun on Privacy:: Get over it. In: *Wired* [online]. 1999 [cit. 2017-07-11]. Dostupné z: https://www.wired.com/1999/01/sun-on-privacy-get-over-it/
- SUROWIECKI, James. The Collective Intelligence of the Web. In: *The New Yorker* [online]. 2014 [cit. 2017-07-11]. Dostupné z: http://www.newyorker.com/tech/elements/the-collective-intelligence-of-the-web
- ŠABLATURA, Jan. Budete dodržovat „sušenkový zákon“? A je to vůbec možné? In: *Zdroják* [online]. 2015 [cit. 2017-07-11]. Dostupné z: https://www.zdrojak.cz/clanky/budete-dodrzovat-susenkovy-zakon-je-vubec-mozne/
- Kallmeyer, W. & Schütze, F. 1976. Konversationsanalyse. Studium Linguistik, 1, 1–28.
- ŠKORNIČKOVÁ, Eva. *GDPR: Obecné nařízení o ochraně osobních údajů* [online]. Praha, 2016 [cit. 2017-07-11]. Dostupné z: https://www.gdpr.cz.
- ŠVAŘÍČEK, Roman a Klára ŠEĎOVÁ. *Kvalitativní výzkum v pedagogických vědách*. Praha: Portál, 2007. ISBN 978-80-7367-313-0.
- Radbâţă, A. 2011. Internet User Behavior. *Bulletin Of The Transilvania University Of Brasov. Series V: Economic Sciences.* 2011, **4**(2), 129-136, [cit. 2017-07-11]. Dostupné komerčně z: EBSCOhost.
- BRUWER, R. a R. RUDMAN. 2015. Web 3.0: Governance, Risks and Safeguards. *Journal of Applied Business Research*. 2015, **31**(3), 1037-. ISSN 0892-7626. Dostupné komerčně z: ProQuest Central.
- ROZMAJZL, Lukáš. Jak smazat digitální stopu. In: *Dotyk* [online]. 2014 [cit. 2017-07-11]. Dostupné z: http://www.dotyk.cz/publicistika/jak-smazat-digitalni-stopu.html
- YOUYOU, Wu, Michal KOSINSKI a David STILLWELL. 2015. Computer-based personality judgments are more accurate than those made by humans. *Proceedings of the National Academy of Sciences* [online]. 2015, **112**(4), 1036-1040 [cit. 2017-03-02]. DOI: 10.1073/pnas.1418680112. ISSN 0027-8424. Dostupné z: http://www.pnas.org/lookup/doi/10.1073/pnas.1418680112.
- Verizon. 2015. Web 3.0: Its Promise and Implications for Consumers and Business. Verizon Business. 2015. Dostupné z: http://www.ddwei.info/pdf/WebBusinesses/5.pdf.
- VÝROST, Jozef a Ivan SLAMĚNÍK. 2008. *Sociální psychologie*. 2., přeprac. a rozš. vyd. Praha: Grada, 2008. Psyché (Grada). ISBN 978-80-247-1428-8.
- W3C. 2015. Semantic web. In: W3C. *W3C* [online]. Keio, 2015 [cit. 2017-07-11]. Dostupné z: https://www.w3.org/standards/semanticweb.

- WATSON, Sara M. How to take control of your online advertising profile. In: *Aljazeera America* [online]. 2014 [cit. 2017-07-11]. Dostupné z: http://america.aljazeera.com/articles/2014/9/22/controlling-onlineadvertising.html.
- WILLIAMS, James. Introducing The Concept Of Web 3.0. In: *Teak and Trick* [online]. 2017 [cit. 2017-07-11]. Dostupné z: http://www.tweakandtrick.com/2012/05/web-30.html.
- WHITE, David S. a Alison LE CORNU. Visitors and Residents: A new typology for online engagemen. *First Monday* [online]. 2011, **16**(9) [cit. 2017-07-11]. ISSN 1396-0466. Dostupné z: http://firstmonday.org/ojs/index.php/fm/article/view/3171/3049.
- WHO. 2011. *Standards and Operational Guidance for Ethics Review of Health-Related Research with Human Participants*. 1. Ženeva: WHO Press, 2011. ISBN 978-92-4-150294-8.
- XIA, Feng, Laurence T. YANG, Lizhe WANG a Alexey VINEL. Internet of Things. *International Journal of Communication Systems* [online]. 2012, **25**(9), 1101-1102 [cit. 2017-07-11]. DOI: 10.1002/dac.2417. ISSN 10745351. Dostupné z: http://doi.wiley.com/10.1002/dac.2417.

Seznam obrázků

Seznam grafů

Seznam tabulek

Přílohy

Příloha č. 1

Ahoj,

jmenuji se Michaela Pappová, studuji na ústavu informačních studií a knihovnictví FF UK. Na začátek bych se ráda zeptala, zda bude v pořádku, když ti budu během rozhovoru tykat? Samozřejmě ty mi můžeš tykat také.

Tento rozhovor bude podkladem pro mou diplomovou práci, která se zabývá tím, jak studenti nakládají se svou digitální stopou. Pokud zrovna nevíš, co si pod pojmem digitální stopa představit, tak si to ujasníme během rozhovoru.

Při tomto rozhovoru je uplatňováno zajištění plné anonymity, tvoje jméno nebo jakékoliv jiné osobní údaje nebudou nikde uvedeny. Identifikovat tě budu číslem.

Rozhovor je členěn do tří částí a obsahuje zhruba dvacet základních otázek. Bude trvat kolem 45 minut. Rozumím tomu, že je to poměrně dlouhá doba, a poskytnutí tvého času si velmi cením. Pokud ti to nebude vadit, pořídila bych si pro lepší zachycení tvých odpovědí audio nahrávku. Zároveň si budu dělat poznámky a klást ti doplňující otázky. Prosím abys odpovídal/a upřímně a podle toho, jak se zrovna cítíš, neexistují špatné ani dobré odpovědi. Kdyby ti vadilo o čemkoliv mluvit, klidně mi řekni a můžeme se k danému tématu postavit jinak nebo jej zcela vynechat. Zároveň pokud bys ses na něco chtěl/a zeptat mě nebo ti některá otázka nebyla jasná, ptej se.

Chceš se zeptat na něco ještě před začátkem? … Tak výborně, děkuji a přistoupíme k první otázce.

Na začátek několik krátkých informací o tobě.

	Úvod	
	Pohlaví:	
	Věk:	
	Studium:	
	Město:	
	Jak bys hodnotil svoji úroveň práce s informačními technologiemi? - *pomocná škála: základní, uživatelská, nadstandardní uživatelská, administrátorská*	

	AKTIVITA *cílem je zajistit uživatelské pozadí respondenta a jeho běžnou činnost online*	
	Používáš stolní počítač či notebook?	

	Používáš chytrý telefon, tablet nebo jiné podobné zařízení? Přes které z těchto zařízení využíváš připojení k internetu? Jak často se připojuješ? - *Využíváš mobilní data?* - *Pokud ano, jsi online stále?*	
	Používáš aktivně e-mail? U jakého poskytovatele? Používáš aktivně nějaký messanger? Jaký? Telefonuješ přes internet (skype, G+ Hangouts)? Jak využíváš cloud?	
	K čemu využíváš sociální sítě? - *Odkud (z jakého zařízení) je využíváš?* - *Jaké sítě aktivně používáš?* - *Jaká je tebou preferovaná sociální síť?* - *Máš účet na některých, které aktivně nevyužíváš?* - *Publikuješ příspěvky?* - *Hraješ hry?* - *Jaké lidi si přidáváš do přátel/kruhů?*	
	Jak (k čemu) používáš mobil? - *Sdílíš obrázky, fotografie…?* - *Jaké aplikace používáš?* - *Jak často jsi online?* - *Máš zapnuté určování polohy?*	
	Vytváříš aktivně nějaký obsah na internetu? - *Vedeš si blog?* - *Komentuješ články?* - *Diskutuješ na fórech?* - *Jak se nejčastěji přihlašuješ na podobných serverech (přezdívka, facebook účet, e-mail)?*	
	Jak vyhledáváš na internetu informace? - *Odborné informace?* - *Jaké používáš vyhledávače?*	

	Jak jinak ještě využíváš internet? - *Nakupuješ přes internet?* - *Hraješ hry?* - *Díváš se na televizi?* - *Používáš televizi či herní konzoli s připojením na internet?*	

	VĚDOMÍ A DŮVĚRA *cílem je rozdělit respondenty dle míry znalosti*	
	Co si myslíš, že je digitální stopa? - *Co všechno obsahuje?* - *Kdo nebo co ji tvoří?* - *Kdo ji ukládá?* - *Je k tomu, aby zanechával nějakou stopu nutné, abys byl připojen k internetu?* - *K čemu si myslíš, že slouží cookies?* - *Říká ti něco pojem big data?* - *Uvědomuješ si, že tvoje DS vzniká i sledováním tvého chování na mobilu, přes sociální sítě, google, atd.?*	
	V případě, že respondent nemá žádné tušení, volně nastínit, co pojem představuje: *"Je to tvoje stopa v digitálním prostředí. Vytváříš ji aktivně ty i každý, kdo se o tobě zmíní.* ***Vzniká však i bez tvého vědomí, skrz mobilní zařízení, aplikace či programy****…"*	
	Jak může být digitální stopa použita? - *Jak ti může být ku prospěchu?* - *Vnímáš to, že je ti navrhován obsah dle tvého chování?*	

	Jak si nejlépe zabezpečit svoji digitální stopu?
	- *Jak co nejlépe zabezpečit účet např. na sociální síti?*
	- *Co se týče hesla?*
	  - *Jak si představuješ silné heslo?*
	- *Připadá ti nutné vědomě tato data zabezpečovat?*
	- *Víš o nějaké legislativě, která tuto ochranu zajišťuje?*
	- *Jaké informace, které o sobě lidé sdílí online, mohou být zneužity?*
	  - *Jak mohou být zneužity?*	

	Znáš nějaké nástroje proti vytváření a využití digitální stopy? - Doplňky do prohlížeče?	

	- K čemu přesně tyto nástroje slouží? - K čemu si myslíš, že souží anonymní režim v prohlížeči?	

	OVLIVNĚNÍ *cílem je rozdělit respondenty dle jejich chování ke své digitální stopě*	
	Jak máš nastavené soukromí na preferované sociální síti (doplnit nejvíce používanou z úvodu)? - *Co se stane po zrušení účtu na preferované sociální síti?* - *Máš účet "na Google" (email, G+)?* - *Jak tam máš nastavené soukromí?* - *Nastavuješ si soukromí ještě na nějaké jiné síti?* - *K čemu všemu povoluješ přístup nainstalovaným aplikacím na mobilu?*	.
	Myslíš si, že informace, které jsi po sobě nějakým způsobem zanechal na internetu, jsou v bezpečí? - *Když se registruješ např. na sociální síti, důvěřuješ, že data, která stránce svěříš, nezneužije?* - *Čteš si obecně obchodní podmínky?* - *Co bys ze zásady internetu nesvěřil?* - *Jaká rizika mohou plynout z tvé digitální stopy?* Přijde ti celkově, že se na internetu chováš tak, že jsou tvá data v bezpečí? - *V čem bys chtěl svoje chování změnit?*	
	Zjišťuješ si aktivně svoji digitální stopu? - *(ano) Jak?* - *(ne) Proč?*	
	Jak se na internetu prezentuješ? - *Seberealizuješ se na internetu?* - *Jsou informace, které uvádíš na (FB, blog, atd) pravdivé?* - *Co si myslíš, že by si někdo o tobě pomyslel, kdyby si tě vyhledal na internetu (vyhledávač lidí, běžný vyhledávač, sociální sítě)?* - *K čemu si myslíš, že ti tvá internetová identita je?* - *Chtěl bys, aby ti k něčemu byla?* - *Jsou lidé dostatečně opatrní a zodpovědní při tvorbě digitálních stop ostatních?* - *(Pokud má nějaký "veřejný zájem" - chceš, aby tvá veřejná identita byla spojena s tvou soukromou?)*	
	Hlídáš si cíleně svoje chování online? - *Používáš pro většinu služeb stejné heslo?* - *Kolik různých přezdívek používáš?* - *Jakým způsobem si pamatuješ přihlašovací údaje do různých služeb?* - *Jak často publikuješ na sociálních sítích?* - *Jak zaměřené jsou příspěvky, které uveřejňuješ?*	

	- *Jsou veřejné?* - *Máš zalepenou kameru či mikrofon?*	
	Používáš nějaké nástroje, které by měly zabránit jakékoliv třetí straně ukládat o tobě data? - *Jaké?* - *Proč?* - *Vyvíjíš nějaké jiné snahy o to, aby tvůj přístup na internet byl co nejvíce anonymní?*	
	Jaká pozitiva plynou z toho, že je tvoje digitální stopa ukládána třetími stranami? - *Jaká negativa?*	
	Přijde ti důležité se zajímat o tvoji digitální stopu? - *Přijde ti tvoje znalost tématiky dostatečná?* - *Budeš se dál nějak rozvíjet?* - *Absolvoval jsi někdy nějakou vzdělávací akci/přednášku o této tématice?* - *Vyhledával sis někdy cíleně informace o této tématice?*	

ZÁVĚR

- Myslíš si, že tento rozhovor nějak změnil tvé vnímání tématiky digitálních stop?
- Chtěl/a bys mi ještě něco říct k digitální stopě?

Děkuji za tvůj čas a tvé odpovědi. Pokud budeš chtít a dáš mi na sebe kontakt, mohu ti zaslat finální verzi diplomové práce nebo krátké shrnutí výsledků výzkumu.